

White Paper



Author: John Bernard

AAEON Technology Inc.

August, 2026

Secure-by-Design

Navigating the EU Cyber Resilience Act (CRA)

Contents

Executive Summary	- 3 -
Understanding the EU Cyber Resilience Act	- 4 -
What Is the EU Cyber Resilience Act?	- 4 -
Key Cybersecurity Requirements.....	- 4 -
Impact on Suppliers, System Integrators, and the Supply Chain	- 5 -
Product Categories and Conformity Assessment	- 7 -
CRA Timeline and Compliance Milestones	- 8 -
The Synergy Between CRA and IEC 62443-4-1	- 9 -
Different Frameworks, Shared Security Principles.....	- 9 -
Secure Development Lifecycle as the Common Foundation.....	- 10 -
How AAEON Helps Customers Prepare for the CRA.....	- 11 -
IEC 62443-4-1 Maturity Level 2 Certification	- 11 -
Security-by-Design Across the Product Lifecycle	- 12 -
SBOM and Third-Party Component Management	- 12 -
Pre-Compliance Assessment and Documentation Support.....	- 13 -
Building a Stronger Foundation for CRA Readiness	- 14 -
About AAEON	- 15 -
Disclaimer	- 15 -

Executive Summary

Cybersecurity threats are no longer solely a traditional IT infrastructure concern. The increasingly interconnected nature of digital ecosystems means that vulnerabilities present in third-party components or open-source software can serve as entry points for malicious actors.

To combat this and establish a unified framework that will institute mandatory cybersecurity requirements for products with digital elements, Regulation (EU) 2024/2847, also known as the European Union's Cyber Resilience Act (CRA), will be fully applicable from 11 December 2027.¹

The CRA has substantial implications for system integrators and manufacturers, given their final products typically include a range of third-party components. The robustness of platform and component suppliers' security practices will therefore influence the conformity of a finished product.² Because of this, supplier selection is likely to become an important part of manufacturers' own cybersecurity and compliance strategies.

It is at this point that international cybersecurity standards such as IEC 62443-4-1 become relevant. While IEC 62443-4-1 and the CRA are distinct frameworks, and IEC 62443-4-1 certification does not inherently guarantee CRA compliance, embedded platform providers already operating under an independently assessed secure development framework are in a position to provide customers with a credible base from which to address their own cybersecurity and compliance obligations.

AAEON has taken this step by achieving IEC 62443-4-1 certification for its Product Security Development Lifecycle Process, demonstrating to its customers that security has been incorporated into the processes governing how products are developed and maintained. In addition to this, AAEON has committed to instituting a practical product security and compliance support framework to proactively reduce the workload required for customers to pursue appropriate third-party conformity assessments.³

This white paper examines the implications of the CRA for system integrators and solution builders, explores the areas of alignment between the CRA and IEC 62443-4-1, and examines how AAEON's CRA preparation goes further than IEC 62443-4-1 certification, introducing new initiatives to assist customers preparing their own products and processes for the evolving cybersecurity requirements of the European market.

¹ Regulation (EU) 2024/2847, Article 71(2).

² Regulation (EU) 2024/2847, Article 13(5); Recital 34.

³ Regulation (EU) 2024/2847, Article 32(1)–(3).

Understanding the EU Cyber Resilience Act

What Is the EU Cyber Resilience Act?

The EU Cyber Resilience Act (CRA) is a comprehensive legal framework introduced to establish horizontal cybersecurity requirements that address known and potential vulnerabilities related to products with digital elements placed on the European Union market.⁴

A key facet of the Act is that it accounts for the evolving nature of connected technologies and the intricate supply chain involved in bringing products with digital elements to market. As such, a cornerstone of the Act is to address the issue of cybersecurity throughout the entire product lifecycle.⁵ Under the CRA, manufacturers must maintain and monitor their security practices from product planning and design through post-market vulnerability monitoring, thus increasing the overall level of cybersecurity of products with digital elements placed on the EU market.⁶

Approaching cybersecurity from the lens of a product's entire lifecycle is particularly relevant to embedded computing. Products with digital elements can contain a variety of constituent parts. For example, applications will typically include hardware, firmware, operating systems, drivers, third-party software, and open-source components manufactured or developed by different suppliers. The security of a fully deployed solution can subsequently depend on how closely entities throughout the supply chain adhere to security practices.

The CRA therefore shifts cybersecurity responsibility further upstream, making secure development practices and supplier due diligence vital considerations when selecting the platforms and components used to build products for the European market.⁷

Key Cybersecurity Requirements

The scope of the CRA is broad, extending to entities across the supply chain. However, the primary requirements as they pertain to manufacturers relate to establishing and maintaining cybersecurity practices throughout the product lifecycle, from secure-by-design development and cybersecurity risk assessment through vulnerability handling, security updates, documentation, and post-market monitoring.

⁴ Regulation (EU) 2024/2847, Article 1(a).

⁵ Regulation (EU) 2024/2847, Article 1(b)–(c) and Article 13(2).

⁶ Regulation (EU) 2024/2847, Article 13(2); Article 13(7)–(9); Annex I Part II.

⁷ Regulation (EU) 2024/2847, Article 13(5).

- Incorporate cybersecurity measures throughout the full product lifecycle, from planning, design, development, and verification through production and maintenance to ensure products entering the market are secure by default, incorporating necessary cybersecurity measures, including measures to minimize attack surfaces and prevent known exploitable vulnerabilities⁸.
- Perform cybersecurity risk assessments, the results of which are to be considered during product planning, design, development, production, delivery, and maintenance, effectively bonding engineering decisions with regulatory obligations.⁹
- Ensure that vulnerabilities can be addressed through security updates and maintain processes capable of responding to newly discovered vulnerabilities throughout the applicable product support period.¹⁰
- Report actively exploited vulnerabilities and severe incidents that impact a product's security, and implement risk mitigation and corrective measures to address identified security risks.¹¹

Impact on Suppliers, System Integrators, and the Supply Chain

Who is Impacted?

Because products with digital elements are often made up of hardware, firmware, and software from multiple parties, organizations that integrate embedded computing platforms with their own software or components and place the resulting product on the EU market under their own name or trademark may fall within the CRA's definition of a manufacturer and become subject to the Act's corresponding obligations.¹²

In such instances, compliance extends beyond the security of the organization's own software and development practices. The security practices of upstream third parties can also influence the cybersecurity posture of the finished product. Vulnerabilities in hardware, firmware, operating systems, drivers, third-party software, or open-source components may introduce or contribute to risks in finished products.

⁸ Regulation (EU) 2024/2847, Article 13(1); Annex I, Part I(a), (b) and (j).

⁹ Regulation (EU) 2024/2847, Article 13(2).

¹⁰ Regulation (EU) 2024/2847, Article 13(7)-(9); Annex I, Part I(c); Annex I, Part II(2).

¹¹ Regulation (EU) 2024/2847, Article 14(1)-(3), and (8).

¹² Regulation (EU) 2024/2847, Article 3(13); Article 20.

Penalties for Non-Compliance

The CRA provides clear guidelines on the penalties that may be imposed on entities for non-compliance, with severity determined by the provision that such an entity fails to comply with. The most notable of these relates to compliance with the essential cybersecurity requirements of the Act, outlined in the Key Cybersecurity Requirements section of this white paper. This penalty is €15,000,000, or up to 2.5% of worldwide annual turnover for the preceding financial year in cases where the offender is an undertaking.¹³

Meanwhile, improper reporting, deemed as providing “incomplete or misleading information” to notified bodies or market surveillance authorities carries administrative fines of up to €5,000,000, or up to 1% of worldwide annual turnover for the preceding financial year in cases where the offender is an undertaking.¹⁴

Ensuring compliance with respect to the CRA’s requirements regarding both pre and post-market cybersecurity considerations and reporting procedures will therefore be a priority for organizations throughout the embedded computing industry.

Impact on Upstream Vendor Selection

It follows that because the scope of responsibility has expanded, supplier selection and due diligence are likely to become vital to system integrators. While factors such as the relationship an organization has with its vendors, product fit, and price will remain key decision drivers, the robustness of a supplier’s cybersecurity practices will likely become a part of this decision-making matrix.

This shift toward upstream cybersecurity also creates opportunities for embedded computing platform providers. For instance, if such a provider can demonstrate that its platforms are developed and maintained under a structured and independently assessed security development process, it can provide downstream customers with a stronger foundation for addressing their own cybersecurity and conformity assessment requirements.

Additional services, such as pre-compliance testing and verification by companies recognized by CRA Notified Bodies, can further provide customers with technical evidence and documentation to

¹³ Regulation (EU) 2024/2847, Article 64(2).

¹⁴ Regulation (EU) 2024/2847, Article 64(5).

support their own conformity assessment activities for the purposes of accelerating the market readiness of finished products.

Product Categories and Conformity Assessment

The CRA categorizes products with digital elements as Important or Critical based on their potential cybersecurity risk and core functionality. For example, an embedded platform containing an operating system or processor listed in Annex III does not automatically become an Important Product simply because it incorporates such a component.¹⁵

Class	Examples	Typical conformity route
Default/Other Products with Digital Elements	Most products with digital elements not classified as Important or Critical	Internal control/self-assessment, subject to applicable CRA requirements. ¹⁶
Important; Class I	Password managers, VPN products, network management systems, operating systems	Internal control where the applicable harmonized standards, common specifications, or cybersecurity certification schemes meet the CRA conditions; otherwise third-party assessment. ¹⁷
Important; Class II	Firewalls, IDS/IPS, hypervisors, tamper-resistant microprocessors	Third-party assessment or applicable cybersecurity certification. ¹⁸
Critical	Smart meter gateways, smartcards, secure elements	Third-party assessment via a notified body; European cybersecurity certification where required under the applicable CRA provisions. ¹⁹

Given the range of components used by system integrators to develop a final product, ascertaining conformity assessment requirements can be a complex task. There are also important caveats that need to be remembered, such as the fact that the classification and conformity assessment requirements of a finished product are determined by the finished product's own characteristics and core functionality (where relevant), not inherited from the classification of its constituent parts.

Therefore, while an AAEON single-board computer may incorporate components with security-related functions, such as an onboard TPM 2.0 security component, the board itself is not automatically classified as an Important Product.

¹⁵ Regulation (EU) 2024/2847, Article 7(1); Annexes III–IV.

¹⁶ Regulation (EU) 2024/2847, Article 32(1).

¹⁷ Regulation (EU) 2024/2847, Article 32(2).

¹⁸ Regulation (EU) 2024/2847, Article 32(3).

¹⁹ Regulation (EU) 2024/2847, Article 8(1), Article 32(3); Annex IV.

Conversely, many general-purpose embedded computing platforms, depending on their specific functionality and configuration, will generally fall within the default/other products with digital elements category by virtue of their core functionality not corresponding to an Important or Critical Product category identified by the CRA. However, downstream integrators need to be mindful not to accept that this classification carries over to a final product that incorporates them, regardless of how central the AAEON platform may be to the function of the resulting system.

CRA Timeline and Compliance Milestones

The CRA entered into force in December 2024. However, its provisions are being implemented in stages in order to give organizations time to align their product development, cybersecurity, vulnerability management, and conformity assessment processes with its requirements. The majority of the CRA will apply from 11 December 2027, with certain provisions applying earlier.

- **10 December 2024 – CRA entered into force**

Regulation (EU) 2024/2847 entered into force on 10 December 2024, beginning the transition period before its main requirements apply.²⁰

- **11 June 2026 – Conformity assessment body notification provisions begin to apply**

Chapter IV (Articles 35 to 51), which relates to the notification of conformity assessment bodies, applies from 11 June 2026.²¹ This stage allows the assessment infrastructure required by the CRA to be established ahead of the regulation's broader application.

- **11 September 2026 – Vulnerability and incident reporting becomes mandatory**

Article 14 will apply from 11 September 2026, meaning that manufacturers will have a legal obligation to report actively exploited vulnerabilities and severe incidents that affect the security of products with digital elements.²² By this date, manufacturers will therefore need to have established internal vulnerability monitoring, incident assessment, and timely reporting processes in place.

- **11 December 2027 – Main CRA requirements apply**

The CRA's main provisions will become fully applicable on 11 December 2027.²³ From this date, the regulation's principal requirements will apply to products with digital elements within the Act's scope, including requirements relating to cybersecurity throughout the product lifecycle, vulnerability handling, security updates, technical documentation, and

²⁰ Regulation (EU) 2024/2847, Article 71(1).

²¹ Regulation (EU) 2024/2847, Article 71(2).

²² Regulation (EU) 2024/2847, Article 71(2); Article 14(1)–(3), (8).

²³ Regulation (EU) 2024/2847, Article 72(2).

conformity assessment. Products placed on the EU market will need to comply with the applicable CRA requirements.

For manufacturers and system integrators, it is important that 11 December 2027 is not seen as the finishing line with respect to CRA obligations. Instead, adherence to the Act's principal requirements as they relate to secure development, vulnerability management, documentation, supply-chain, and conformity assessment processes should be considered an ongoing process present throughout an organization's operation.

The Synergy Between CRA and IEC 62443-4-1

Different Frameworks, Shared Security Principles

The CRA represents a significant development in regulating how cybersecurity is managed by manufacturers of products with digital elements, but an established international cybersecurity standard already exists. Albeit within a different regulatory context, the Secure Product Development Lifecycle (SDL) standard, or IEC 62443-4-1, is an international standard that defines secure development lifecycle (SDL) requirements.

Despite the differences in regulatory contexts, the cybersecurity principles of the two frameworks overlap. IEC 62443-4-1, by its very nature, focuses heavily on security from the very beginning of product development. It also shares the CRA's recognition of the need for manufacturers to have robust methods through which to mitigate cybersecurity vulnerabilities, provide security updates, include risk assessments as part of their decision-making processes, and maintain high security standards throughout the product lifecycle.

Because of these shared principles, a manufacturer with an IEC 62443-4-1-certified process can be a useful factor for system integrators to include in their supplier selection decision-making. In short, a system integrator may reasonably view a manufacturer operating under an independently assessed IEC 62443-4-1 process as having already adopted many of the organizational and engineering practices that support corresponding CRA requirements.

Despite their shared security principles, IEC 62443-4-1 should not, however, be regarded as an alternative to the conformity assessment procedures set out by the CRA.²⁴ Rather, IEC 62443-4-1's

²⁴ Regulation (EU) 2024/2847, Article 32.

secure development practices framework can provide a structured base on which manufacturers and system integrators can build processes that address relevant CRA cybersecurity requirements.

Secure Development Lifecycle as the Common Foundation

The overlap between aspects of the CRA and IEC 62443-4-1 is most readily apparent with their shared treatment of cybersecurity as a lifecycle responsibility, rather than a single quality assurance measure.

This is best illustrated by outlining the requirements that are evaluated during IEC 62443-4-1 process conformity assessment, which covers 47 requirements across eight main areas.²⁵

IEC 62443-4-1 Area	Evaluation Criteria
Security Management (SM)	Whether the organization has an established secure development cycle, defined responsibilities and security expertise, secure development processes and environments, controls for externally provided components, security issue processes, verification, and continuous improvement.
Specification of Security Requirements (SR)	Whether security requirements are systematically established from the product's context and threat model, documented, and reviewed.
Secure by Design (SD)	Whether security is incorporated into product architecture and design through secure design principles, defense-in-depth, design reviews, and established secure-design practices.
Secure Implementation (SI)	Whether implementation is subject to security review and secure coding standards.
Security Verification & Validation (SVV)	Whether security requirements and threat mitigations are tested, including vulnerability and penetration testing, with appropriate tester independence.
Management of Security-Related Issues (DM)	Whether the organization has processes to receive, review, assess, address, disclose, and periodically review security-related issues.
Security Update Management (SUM)	Whether security updates are qualified, documented, delivered, and provided in a timely manner, including consideration of dependent components and operating systems.
Security Guidelines (SG)	Whether customers/users receive guidance for securely configuring, operating, hardening, managing accounts, disposing of, and maintaining the product.

As is evidenced by the breadth of these requirements, IEC 62443-4-1 evaluates how deeply security is embedded in an organization's product development lifecycle process. The eight main areas covered by IEC 62443-4-1 resemble many of the objectives emphasized by the CRA, with proactive security management throughout product planning, development, production, delivery, and post-

²⁵ IEC 62443-4-1:2018, Practices 1–8 (Sections 5–12).

market support standing out. That said, it is important not to conflate the two and assume the frameworks are interchangeable.

For a supplier like AAEON, having its product security development process independently assessed against IEC 62443-4-1 provides its customers with evidence that cybersecurity has been embedded into the development process at an institutional level, rather than treated solely as a product-level feature or a final compliance exercise. The controls assessed across its eight areas can therefore be an insightful benchmark for system integrators to use when evaluating suppliers and developing their own cybersecurity and compliance processes.

How AAEON Helps Customers Prepare for the CRA

IEC 62443-4-1 Maturity Level 2 Certification



AAEON initiated efforts to obtain IEC 62443-4-1 certification in June 2025, in preparation of the CRA becoming fully applicable. Working alongside independent consulting firms, AAEON proactively reviewed its existing Product Security Development Lifecycle Process V1.0, as well as undertaking both independent and internal reviews.

During this period, AAEON implemented detailed standardized procedures, such as security management documentation and supporting forms, while also undertaking comprehensive internal security awareness training programs.

Following a Process Capability Assessment conducted by LCIE (Laboratoire Central des Industries Électriques) under the IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE), AAEON achieved IEC 62443-4-1 Maturity Level 2 certification for its Product Security Development Lifecycle Process V1.0.²⁶

The assessment evaluated all 47 requirements across the Security Management (SM), Specification of Security Requirements (SR), Secure by Design (SD), Secure Implementation (SI), Security Verification & Validation (SVV), Management of Security-Related Issues (DM), Security Update Management (SUM), and Security Guidelines (SG) areas.

²⁶ LABORATOIRE CENTRAL DES INDUSTRIES ELECTRIQUES (LCIE), *Certificate of Conformity – Industrial Cyber Security Capability*, Ref. Certif. No. FR_Cyber10305, AAEON Product Security Development Lifecycle Process Version V1.0, IEC 62443-4-1:2018, 22 May 2026.

Achieving IEC 62443-4-1 Maturity Level 2 certification was not the end goal, but one part of AAEON's proactive efforts to provide its customers with greater visibility and transparency regarding its organizational security practices.

The certification does not, however, constitute CRA conformity or transfer the responsibility for assessing a customer's finished product to AAEON. Rather, it provides one component of the broader support AAEON can offer customers preparing products for the EU market under the CRA.

Security-by-Design Across the Product Lifecycle

Under AAEON's Product Security Development Lifecycle Process V1.0, implementation of IEC 62443-4-1 commences at the very beginning of development. As part of this, security requirements are integrated into Product Requirements Documents (PRDs) and Software Requirements Specifications (SRSs), meaning that cybersecurity is considered as part of a product's functional and technical requirements from the outset. Secure code review is also incorporated into the development process to identify and address potential security weaknesses that could be vulnerable to exploitation during or following implementation.

AAEON's Product Security Development Lifecycle Process V1.0 also establishes product-level security requirements, including security update capabilities and supply chain security requirements. These measures have been put in place to extend security as a factor beyond product development, instead making it something that can be maintained throughout the applicable support lifecycle. For AAEON customers, this approach provides greater visibility into how security is incorporated into the embedded platforms they integrate into their own final products.

SBOM and Third-Party Component Management

AAEON's embedded platforms support a broad range of operating systems, software development kits, and firmware from multiple third-party providers. For example, the board support package (BSP) for its embedded AI system series comes with a range of preinstalled NVIDIA Jetpack™ software development kit components.

Meanwhile, products based on Intel® processing platforms, such as AAEON's developer board series, often provide dedicated software packages, OS images, and drivers. As such, understanding the software composition of its products is an important part of how AAEON manages cybersecurity risk.

Operating systems, drivers, libraries, firmware, and other software components all have the potential to introduce vulnerabilities that may affect a product. By maintaining up-to-date information about these components, AAEON positions itself as better able to identify vulnerabilities and respond efficiently to them.

As part of AAEON's Product Security Development Lifecycle Process V1.0, a Software Bill of Materials (SBOM) is established during the design phase, including the registration of third-party components incorporated into products under development. Beyond this, Continuous Integration/Continuous Delivery (CI/CD) has been used to implement an automated SBOM generation process in order to maintain component information, reducing the risk of SBOM information becoming inaccurate or outdated. This approach is also aligned with the CRA's requirements on the identification and documentation of software components and vulnerabilities, including through the use of SBOMs.²⁷

In addition to SBOM management, AAEON also conducts product security testing, such as firmware security testing, SBOM verification, and CVE (Common Vulnerabilities and Exposures) tracking. These activities provide mechanisms through which potential third-party component vulnerabilities can be identified, while also ensuring that the software composition recorded for a product accurately reflects its implementation. Together with product-level security requirements covering security updates, these processes support the ongoing management of software supply-chain risks throughout the applicable support lifecycle.

Pre-Compliance Assessment and Documentation Support

As part of its customer-centric approach, AAEON maintains a philosophy of institutional agility. This principle is most visible in its commitment to helping customers bring finished products to market through the provision of flexible customization services that include schematic review, design consulting, and customized product development tailored to address specific project needs.

Recognizing that system integrators and solution builders remain responsible for assessing the conformity of their own finished products, AAEON has expanded the services it can offer to customers to support their own CRA preparation and conformity assessment activities.

To do this, AAEON is establishing processes that enable it to provide technical evidence, pre-compliance reports, and documentation generated through independent testing and verification

²⁷ Regulation (EU) 2024/2847, Annex I, Part II(1); Annex VII(2)(b).

activities. By providing such materials prior to formal conformity assessment, customers may be able to reduce the testing and documentation workload associated with their own Certification Body (CB) or Verification of Conformity (VoC) processes.

Proactive support from AAEON can therefore potentially improve the market readiness of customers' finished products while helping customers manage the associated certification effort and costs.

Building a Stronger Foundation for CRA Readiness

The CRA will undoubtedly change how cybersecurity is approached by manufacturers placing products with digital elements on the European market. This will apply to both embedded platform providers such as AAEON and the downstream system integrators that utilize embedded platforms as part of their final products.

As this white paper has outlined, cybersecurity no longer sits solely at the product level, but as a consideration throughout product lifecycles across the supply chain. For organizations building finished products from embedded computing platforms and other third-party components, this also makes the security practices of upstream suppliers an important factor in platform selection.

AAEON's IEC 62443-4-1 Maturity Level 2 certification demonstrates that its Product Security Development Lifecycle Process V1.0 has already been independently assessed against an international secure development framework with requirements that align closely with those of the CRA. However, AAEON's CRA preparations extend beyond the development and maintenance of its own platforms.

By establishing initiatives and service offerings aimed at assisting customers with their own CRA preparation and conformity assessment activities, AAEON is in a position to provide system integrators with technical evidence and practical support as they prepare final products for introduction into the European market. In doing so, AAEON aims to make the cybersecurity and conformity assessment aspects of global projects more predictable and manageable, while helping customers retain responsibility for meeting the requirements applicable to their own finished products.

About AAEON

Established in 1992, AAEON is one of the leading designers and manufacturers of industrial IoT and AI Edge solutions. With continual innovation as a core value, AAEON provides reliable, high-quality computing platforms including industrial motherboards and systems, rugged tablets, embedded AI Edge systems, uCPE network appliances, and LoRaWAN/WWAN solutions. AAEON also provides industry-leading experience and knowledge to provide OEM/ODM services worldwide. AAEON works closely with premier chip designers to deliver stable, reliable platforms. For an introduction to AAEON's expansive line of products and services, visit www.aaeon.com.

Disclaimer

This white paper is provided for informational purposes only and does not constitute legal advice, regulatory advice, or a determination of CRA conformity for any particular product. Manufacturers and other economic operators should assess the requirements applicable to their individual products and circumstances.