ASRock Industrial Cyber Resilience Act (CRA) Compliance White Paper

Published by ASRock Industrial Computer Corp.
Publication Date: July 2026
Updated: September 2, 2026

1. Introduction and Executive Summary

ASRock Industrial is committed to providing secure, trustworthy edge AI computing platforms, and we work closely with global customers to help them build products and solutions to meet international cybersecurity standards and regulatory requirements.

To continuously strengthen product cybersecurity and reinforce trust across our supply chain, ASRock Industrial has built a comprehensive information security governance system and holds the following international cybersecurity certifications:

- **ISO/IEC 27001:2022** – Certification No. 2026/117844.1
  Information Security Management System certification
- **IEC 62443-4-1** – Certification No. NL-103556
  Secure Product Development Lifecycle certification
- **IEC 62443-4-2** – Certification No. NL-113417
  Technical Security certification for Industrial Automation and Control System components
- **FIDO Device Onboard (FDO)** – Certification No. FDO000020240906004
  Secure Device Onboarding certification

This white paper sets out the product security architecture, compliance strategy, and ongoing maintenance mechanisms ASRock Industrial has established in response to the European Union's Cyber Resilience Act (CRA), helping customers address the EU market's cybersecurity regulatory requirements.

2. About the EU Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA) is the European Union's mandatory cybersecurity regulation for Products with Digital Elements (PDEs). It requires manufacturers to implement essential cybersecurity requirements during product design, development, production, and the product support period, and to establish mechanisms for vulnerability management, security updates, and incident reporting thereby strengthening the overall cyber resilience of products.

ASRock Industrial has embedded information security into every stage of the product lifecycle and continues to advance its product security governance in line with CRA requirements. Our core practices include:

- **Security by Design:** we build information security requirements into products from the earliest design and development stages, applying risk analysis, threat modeling, and secure design principles throughout the development process.
- **Security Management Throughout Product Support:** we provide continuous information security maintenance, security updates, and vulnerability patches for the full duration of the product support period, sustaining each product's cybersecurity posture throughout.
- **Vulnerability Handling and Incident Reporting:** beginning September 11, 2026, ASRock Industrial will meet its statutory CRA reporting obligations for actively exploited vulnerabilities and severe security incidents, and will deploy the necessary patches and risk-mitigation measures.

3. Scope of Applicable Products

This white paper covers ASRock Industrial products that contain digital elements, including:

- Industrial & Embedded Motherboards
- Embedded Computer Systems
- Industrial Robust Edge AIoT Platforms

Guided by CRA requirements and product risk classifications, ASRock Industrial continuously carries out product security design, compliance review, and information security operations management across this portfolio.

4. CRA Defense-in-Depth and Compliance Strategy

ASRock Industrial applies a Secure-by-Design framework fully aligned with CRA requirements across the full product journey – from development and design through post-market operations and maintenance.

4.1 Secure Development Lifecycle

ASRock Industrial's secure development lifecycle is certified to IEC 62443-4-1 and continues to align with CRA requirements and the relevant prEN 40000 series of international standards. We have built a comprehensive secure product development process that includes:

- **Risk Assessment & Threat Modeling:** information security risk assessments and threat modeling are performed at the earliest stages of product design to surface potential attack scenarios and feed them directly into design decisions and control measures.
- **Code Security Review and Testing:** we combine static and dynamic application security testing (SAST/DAST) to continuously verify code security throughout development.
- **Software Bill of Materials (SBOM):** we create and maintain SBOMs in SPDX and CycloneDX formats to support vulnerability management and supply chain transparency requirements.

4.2 Product Cybersecurity Hardware Design

ASRock Industrial embeds cybersecurity directly into hardware, firmware, and platform architecture. Guided by product-specific cybersecurity risk assessments, we provide security features that support compliance with CRA Annex I, "Essential Cybersecurity Requirements." Key mechanisms include:

- **Hardware Root of Trust:** integrated TPM 2.0 provides hardware-level key protection and boot-integrity measurement, while UEFI Secure Boot verifies each stage of the boot chain so that devices execute only signed, authorized firmware and system software – providing hardware-anchored protection for data confidentiality and system integrity.
- **Trusted Security Updates:** signature verification for firmware and system update images ensures that security updates reach devices reliably and continuously throughout the support period.
- **Reduced Attack Surface, Secure by Default:** products ship in a Secure-by-Default configuration, with unused physical interfaces and debug ports disabled or access-controlled. Devices also support restoration to factory security settings, reducing the product's attack surface throughout the support period.

4.3 Vulnerability Management and PSIRT Mechanism

ASRock Industrial operates a dedicated Product Security Incident Response Team (PSIRT), supported by a comprehensive vulnerability management system that includes:

- **Coordinated Vulnerability Disclosure (CVD):** transparent, ongoing communication with the security research community and prompt remediation of known vulnerabilities.
- **Timely Patching:** security updates delivered promptly, and without undue delay, throughout the support period.

For more information, visit the ASRock Industrial Security Center at https://www.asrockind.com/security-center

5. CRA Compliance Roadmap

ASRock Industrial continues to advance its product security governance in line with CRA requirements, guided by the following roadmap:

Phase	Timeline	Compliance Implementation Details
Phase 1	Completed	Certified to IEC 62443-4-1 / 4-2, establishing ASRock Industrial's secure development and product security capabilities.
Phase 2	Completed	Certified to ISO/IEC 27001:2022, strengthening corporate information security governance and SBOM management processes.
Phase 3	Completed	Building a CRA-compliant vulnerability reporting system and fully operationalizing PSIRT and vulnerability management processes ahead of the reporting obligations

		that take effect in September 2026.
Phase 4	From 2027 (Ongoing Operations)	Establishing sustained cybersecurity operations for products exported to the EU – vulnerability management, security updates, and continuous product security monitoring – to keep products compliant with CRA requirements throughout their support period.

6. Legal Disclaimer and Contact Information

The technical architecture, compliance strategy, timelines, and forward-looking plans described in this white paper are provided for informational purposes only and do not constitute any legal or commercial representation, warranty, or contractual guarantee. Product functional specifications, SBOM delivery methods, cybersecurity update policies, and post-sale support are governed exclusively by the formally executed agreement between the parties, the applicable product specification sheet, and official technical documentation.

For more information about EU CRA regulations or ASRock Industrial's cybersecurity solutions, please contact us:

- Official Website: ASRock Industrial Official Website
- Product and Compliance Inquiries: Product Inquiry