



MEMORANDUM

Nozomi Networks

CRA Compliance

May 2026

Security by Design

The EU Cyber Resilience Act (CRA) sets a new standard for cybersecurity by requiring digital products to be secure by design, resilient by default, and supported throughout their lifecycle. As these requirements come into effect, organizations placing software and connected technologies on the EU market must demonstrate strong security practices, effective vulnerability management, and timely updates.

Nozomi Networks' cybersecurity solutions are purpose-built to support these objectives, helping organizations protect connected environments, identify and respond to threats, and maintain operational resilience. By enabling deep visibility, continuous monitoring, and proactive risk management across industrial and critical infrastructure systems, Nozomi helps customers strengthen their cyber resilience and align with the expectations introduced by the Cyber Resilience Act—building trust, reducing risk, and supporting a more secure digital ecosystem.

Nozomi Networks' CRA Compliance Program

Nozomi Networks is also assessing its own obligations under the Act. To accomplish that, we have established a dedicated, cross-functional project team focused on CRA compliance. This team is responsible for coordinating governance, engineering, product, and assurance activities to help ensure our products and processes align with CRA requirements.

We also recognize that our customers have obligations under the CRA, and we are committed to supporting their compliance efforts by providing clear documentation, timely security information, and evidence aligned to CRA expectations.

Our CRA Compliance Program

Nozomi Networks has launched a comprehensive, company-wide initiative that integrates CRA requirements with the IEC 62443-4-1 and IEC 62443-4-2 certification framework. This combined program strengthens our secure development lifecycle and enhances the technical security controls across all product lines.

Current Progress

- Our Governance, Risk & Compliance, Product, and Engineering teams are jointly executing a structured multi-year roadmap toward CRA conformity that has as its major milestones:
 - Implementation of technical and procedural requirements for incident notification by September 2026 in alignment with the Act.
 - Full CRA compliance expected by December 2027, subject to confirmation following publication of the final Act and any adjustments to the compliance timeline.
- We are currently engaged with a leading certification body to execute the scope of work, meet the required milestones, and kick off audit activities.
- Our program includes certifying our Secure Development Lifecycle under IEC 62443-4-1 within the next 12 months, followed by technical certification under IEC 62443-4-2 by the end of 2027.

Product Lines in Scope

To support CRA classification and certification, our product families are organized as follows:

- **Managers:**
 - Vantage
 - Central Management Console
- **Sensors:**
 - Guardian
 - Guardian Air
 - Arc
 - Arc Embedded

Our Commitment

We are fully committed to meeting all CRA obligations and ensuring our products are secure by design, resilient by default, and supported throughout their lifecycle.

Karen Meohas
Director of GRC
karen.meohas@nozominetworks.com



Cybersecurity for OT, IoT and Critical Infrastructure

Nozomi Networks protects the world's critical infrastructure from cyber threats.

Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response.

Customers rely on us to minimize risk and complexity while maximizing operational resilience.