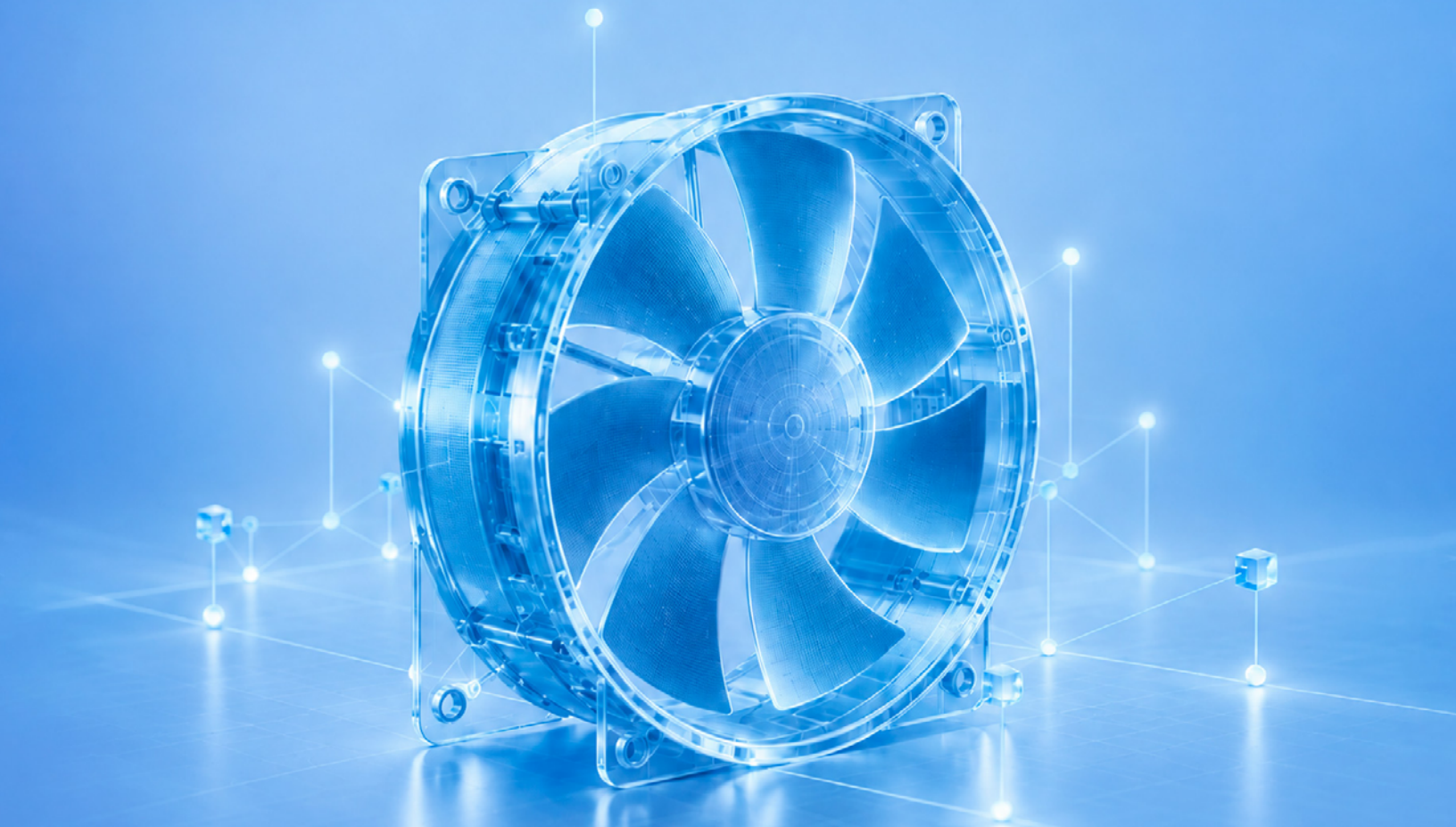
Nemko Digital

CASE STUDY

Building One Scalable CRA Compliance Capability Across a Large Product Portfolio

An industrial manufacturing case study



Executive summary

A world-leading manufacturer of ventilation and connected control technologies needed to translate the EU Cyber Resilience Act (CRA) into a practical operating model for a portfolio of more than 20,000 products. Nemko Digital helped the organization replace fragmented maturity and locally owned processes with one testable compliance program that combines portfolio classification, vulnerability and incident readiness, governance, employee enablement, and traceable evidence. Together with the client, Nemko Digital established a framework for the CRA reporting obligations that apply from September 2026 and built a scalable foundation for the broader product-compliance requirements that apply in 2027.

Section 01

Situation

01

The client operates internationally and manages a highly diverse portfolio spanning fans, embedded firmware, connected gateways, control software, and digital monitoring solutions. Customers and partners increasingly asked about CRA compliance, while business units and technical teams stored product information, assigned responsibilities, and maintained supporting evidence separately. The organization needed a common baseline that could support central governance while accounting for differences in connectivity, software content, operational context, and cybersecurity maturity.

The company had previously established processes to address corporate IT security incidents (e.g., phishing, CEO fraud, and malware). However, product security incident prevention and response remained as gaps.

Section 02

Key Challenges

02

1 Portfolio scale and diversity

The organization manages more than 20,000 products with different software, connectivity, field-access, and deployment profiles.

2 Uneven maturity

Some workstreams followed basic cybersecurity practices, while others needed foundational guidance, ownership, and evidence structures.

3 Regulatory interpretation

The organization needed a consistent way to determine CRA scope, product category, conformity route, and reporting obligations.

4 Fragmented response paths

The organization had not yet connected vulnerability intake, escalation, reporting, remediation, and user communication through one end-to-end process.

4 Federated organization

The organization needed to balance central consistency with enough flexibility for divisions to implement controls in their own product context.

Section 03

Approach

Step 1: Discover, Scope, and Classify

The program began with an onsite headquarters workshop that brought together product, engineering, IT, legal, compliance, and security stakeholders. Nemko Digital mapped CRA obligations to the client's real workflows and decision paths, assessed the current state, and established a high-level roadmap. The team created practical applicability and decision trees for categorization so workstreams assign scope status, identify the likely conformity route, and flag any potentially important or critical products for deeper validation. The assessment placed the portfolio in the CRA default-category self-assessment route and clarified the full scope of CRA requirements.

Step 2: Design the Governance and Reporting Model

Nemko Digital designed a CRA Vulnerability Reporting Standard as the core of the governance and reporting model and guided the client towards internal implementation. Rather than create a disconnected process, the team used the company's existing IT security standards as a baseline and adapted them for product-security and CRA-specific requirements. The team then tailored roles, responsibilities, decision rights, and escalation paths to the organization's operational reality, combining centralized governance and enablement with workstream-level execution and ownership. The standard covered the coordinated vulnerability disclosure program, public reporting-channel requirements, single-point-of-contact criteria, internal escalation, CRA Article 14 decision logic, and 24-hour, 72-hour, and final-report workflows for the ENISA Single Reporting Platform. This approach retained reusable internal controls, filled gaps, and avoided unnecessary duplication.

Step 3: Operationalize, Test, and Build Evidence

The advisory work fit seamlessly to the client's own version-control, documentation, collaboration, and secure-access environments. Nemko Digital guided the client in documenting vulnerabilities and potential security incidents consistently across all workstreams. Hands-on sessions for vulnerability and incident documentation covered product and version identification, affected components, impact and likelihood, exploitation status, evidence, remediation decisions, reporting milestones, user communication, root-cause analysis, and lessons learned. By bringing this information together, the team exposed previously unknown capability gaps in ownership, monitoring, evidence quality, escalation, and remediation tracking. The consolidated view gave the client practical risk context for end-to-end product cybersecurity risk assessments ahead of the December 2027 CRA compliance deadline. Cross-functional workshops helped employees apply the methods consistently, while tabletop exercises and reporting-path rehearsals began testing whether roles, decisions, and evidence would work under real-time pressure.

Section 04

04

Value Delivered

One scalable baseline

The team created a common CRA model that the organization can reuse across more than 20,000 products.

Faster, more consistent decisions

Structured applicability, categorization, risk, and reportability logic reduced reliance on ad hoc interpretation.

Clear accountability

Defined roles, escalation paths, and evidence responsibilities connected central governance with workstream execution.

Operational reporting readiness

The organization gained concrete processes and templates for vulnerability intake, rapid triage, authority notification, remediation, and user communication.

Section 04

04

Audit-ready evidence

Deliverables linked decisions, controls, timestamps, notifications, and remediation records in a traceable compliance model.

Practical organizational adoption

The team integrated guidance into the client's existing documentation and collaboration environment instead of delivering a stand-alone theoretical framework.

Cross-regulatory efficiency

A parallel EU Data Act work package aligned governance, resources, and timelines while preserving separate regulatory scope and deliverables.

The client is taking this project further by testing the reporting process through tabletop exercises, maintaining its vulnerability disclosure channel, and extending the methods to new product families. It also began using consolidated vulnerability, incident, and capability-gap data to inform product cybersecurity risk assessments. In parallel, the client is strengthening lifecycle capabilities for SBOM management, vulnerability monitoring, secure updates, penetration testing, advisories, and post-market evidence, while reinforcing the governance model through training, metrics, management review, and continuous improvement toward full CRA compliance in 2027.

Section 05

05

Final Takeaway

A checklist alone cannot deliver CRA readiness across a large portfolio. Organizations need a repeatable system that connects product classification, cyber risk, vulnerability handling, regulatory reporting, organizational ownership, and evidence. By designing that system around the manufacturer's actual operations, Nemko Digital transformed mixed maturity into one shared compliance capability that the organization can test, improve, and scale.

Nemko
Digital