The Cyber Resilience Act

Why Industrial Organizations Should Pay Attention

Understanding CRA and NIS2: Two EU regulations reshaping vendor-operator relationships and redefining industrial cybersecurity responsibilities.

Published by
Factory Software

Date
February 2026

Table of Contents

1. Introduction
2. Two Regulations, Two Responsibilities
3. Why CRA Compliance Makes Your NIS2 Life Easier
4. What the CRA Actually Requires of Vendors
5. What NIS2 Actually Requires of Operators
6. What Strong Vendor Response Looks Like
7. What This Means for You
8. Building the Foundation for What Comes Next

The email from Procurement seemed routine enough: *"Vendor contract renewal requires updated security attestation. Please confirm all systems meet our current cybersecurity policy."*

Your plant engineer forwarded it to you with a question mark. You're the IT/OT manager for manufacturing operations. You stare at the email for a moment, then open the asset register. The SCADA system was installed in 2011. The historian is from 2008. The edge gateways came with a packaging line you acquired through an M&A deal three years ago, you're not even sure who the original vendor was. Half the OPC servers running in the plant were configured by contractors who are long gone and still rely on DCOM.

You call the vendor. "Can you confirm that our systems meet current cybersecurity standards?" The support engineer is polite but unhelpful. "We can't really speak to how you've configured things. We provided security guidelines in 2011, but we don't know what changes you've made since then. If you want us to audit your environment, that's a separate engagement."

You hang up and realize: nobody actually knows who's responsible for keeping these systems secure. The vendor built them. Your team deployed them. Operations modified them. IT maintains the network they run on. And now Procurement is asking for an attestation that nobody can confidently provide.

This scenario is playing out across industrial organizations right now.

Two new EU regulations are forcing clarity into relationships that have been comfortably vague for decades. The **Cyber Resilience Act (CRA)** defines what vendors must deliver. The **NIS2 Directive** defines what operators must maintain. Together, they're redrawing the line of responsibility for industrial cybersecurity.

Two Regulations, Two Responsibilities

The confusion is understandable, both regulations address cybersecurity, both come from the EU, and both have deadlines soon. But they target different actors and impose different obligations.

CRA

Cyber Resilience Act
The Vendor's Problem (So Our Problem)

It establishes mandatory cybersecurity requirements for digital products sold in the European Union, including industrial software and connected devices. The regulation becomes enforceable in late 2027. Vendors must design products with security built in, maintain security throughout the product lifecycle, provide transparency about software composition, and in many cases obtain CE marking that includes cybersecurity assurance.

NIS2

NIS2 Directive
The Operator's Problem

The Network and Information Security Directive (updated to NIS2 in 2023) requires operators of essential and important services, including manufacturing, energy, water, and critical infrastructure, to implement appropriate cybersecurity measures, report significant incidents, and demonstrate resilience. If you operate industrial facilities in sectors covered by NIS2, compliance is your legal obligation.

Why CRA Compliance Makes Your NIS2 Life Easier

NIS2 requires operators to implement "appropriate and proportionate technical and organisational measures" to manage cybersecurity risks. The directive doesn't prescribe specific technologies or configurations, it establishes outcomes you must achieve. You need to identify vulnerabilities, implement security controls, manage patches and updates, handle incidents effectively, and demonstrate your approach to regulators.

Try doing that with industrial systems built before security-by-design was standard practice. You inherit whatever security posture the vendor provided, plus whatever modifications your team made, plus whatever vulnerabilities emerged since deployment. Patching requires testing and production downtime. Vulnerability management depends on vendor responsiveness. Incident response assumes you have visibility into what's actually running on your systems.

CRA-compliant vendors make this dramatically easier. When vendors build security in from the start, you start with a stronger baseline. When vendors maintain clear vulnerability management processes, you know what risks you're managing. When vendors provide transparent software composition data, you understand your supply chain dependencies. When vendors commit to defined support windows with security updates, you can plan lifecycle management systematically.

The Patch Management Challenge

Consider the patch management challenge. NIS2 expects timely patching of known vulnerabilities. But in industrial environments, patching isn't simple, you need testing windows, production downtime, rollback procedures, and operational validation.

A vendor with mature CRA compliance will provide patches with clear testing guidance, known compatibility constraints, and documented rollback procedures. A vendor treating CRA as checkbox compliance will drop patches over the wall and wish you luck.

Supply Chain Transparency

The supply chain transparency requirement creates even clearer benefits. NIS2 expects you to manage third-party risk. But how do you assess third-party risk when you don't know what third-party components are embedded in your vendors' products?

The CRA forces vendors to document their supply chain dependencies and ensure those components meet security requirements. That documentation becomes your starting point for NIS2 supply chain risk assessment.

The inverse relationship also matters. Organizations demonstrating strong NIS2 compliance will pressure vendors to improve their CRA posture. When you establish clear security requirements for procurement, when you demand transparency about product security, when you hold vendors (that includes us!) accountable for lifecycle support, you're creating market pressure for better vendor practices.

What the CRA Actually Requires of Vendors

Four core requirements shape everything downstream. Products with digital elements must be designed with cybersecurity built in from the start, not bolted on after deployment. Vendors must maintain security throughout the product lifecycle, issuing patches, managing vulnerabilities, documenting security incidents. They must provide transparency about software composition, including third-party components and dependencies. And many products will require CE marking that now signals defined cybersecurity assurance, not just safety conformity.

The Lifecycle Requirement Matters Most

The lifecycle requirement matters most for industrial operations. Unlike consumer software that users replace every few years, industrial systems run for decades. A historian deployed in 2008 is probably still collecting data today. An HMI system from 2012 might control your most critical production line.

The CRA forces vendors to define support windows clearly and maintain security updates throughout those windows. That's a significant shift from the current reality where "end of support" often means "good luck, you're on your own."

For operators facing NIS2 requirements, clear vendor support windows solve a chronic problem. You can't maintain appropriate security measures on systems that vendors no longer support. The CRA gives you leverage: vendors who want to sell in the EU must commit to defined support periods. That commitment enables your NIS2 compliance by ensuring security updates remain available throughout your operational lifecycle.

Supply Chain Ripple Effects

The supply chain transparency requirement creates ripple effects throughout the industry. If your SCADA vendor uses a third-party communication library, that library must also meet CRA requirements. If it doesn't, your vendor needs to replace it or risk non-compliance. This exposes dependencies that have been invisible for years and forces decisions about technical debt that organizations have been postponing.

What NIS2 Actually Requires of Operators

NIS2 establishes a risk management framework rather than prescribing specific controls. Covered entities must assess their cybersecurity risks, implement appropriate measures to manage those risks, and continuously improve their security posture.

The directive identifies specific areas requiring attention:

1. Risk analysis and information system security policies
2. Incident handling
3. Business continuity and crisis management
4. Supply chain security
5. Vulnerability handling and disclosure
6. Measures to evaluate the effectiveness of your approach

The specifics vary by member state, each country implements NIS2 through national legislation that adapts requirements to local context. But the underlying expectations remain consistent: you must demonstrate that you're actively managing cybersecurity risk, that your measures are proportionate to your actual risk exposure, and that you can respond effectively when incidents occur.

For industrial operators, several requirements create immediate challenges. Supply chain security expectations mean you need visibility into vendor practices, third-party dependencies, and the security posture of components you're integrating. Vulnerability handling requires processes for identifying, assessing, and remediating vulnerabilities, which depends on vendors providing timely information and patches. Incident response assumes you have monitoring capabilities, defined escalation procedures, and the ability to contain and recover from security events.

CRA-Compliant Vendors Support Your NIS2 Requirements

Supply chain security gets easier when vendors document their component dependencies. Vulnerability handling gets faster when vendors maintain clear disclosure and patching processes. Incident response gets more effective when vendors provide detailed security documentation and responsive support.

What Strong Vendor Response Looks Like

Not all vendors will approach CRA compliance the same way. Some will do the minimum required to meet regulatory obligations. Others will use CRA as a catalyst for deeper improvements to product development, lifecycle management, and customer support. The difference matters because industrial software isn't just about features, it's about long-term partnership, operational stability, and risk management.

AVEVA has publicly outlined its approach to the EU Cyber Resilience Act, including its commitment to security-by-design practices and lifecycle security. For the latest official guidance, refer to AVEVA's public CRA position.

For operators managing NIS2 compliance, early vendor commitment reduces risk. You can plan upgrades to CRA-compliant versions within your normal maintenance windows rather than scrambling in late 2027. You can align vendor upgrades with other security improvements rather than treating them as isolated compliance projects. And you can demonstrate to regulators that you're proactively managing supply chain risk rather than reacting to deadlines.

Long-Term Servicing Options

The introduction of Long-Term Servicing options addresses a chronic pain point for industrial operators, and directly supports NIS2 compliance. AVEVA now offers two support tracks: Standard Term Servicing with three years of active support plus two years of extended support, and Long-Term Servicing with five years of active support plus two years of extended support. This gives operations teams predictable upgrade windows and longer operational stability, which aligns with how industrial systems actually run.

From an NIS2 perspective, clear support windows solve the "unsupported system" problem. You can't maintain appropriate security measures on systems vendors no longer support. With defined LTS options, you can plan lifecycle management systematically: deploy on LTS track, stabilize and optimize, run for five years with security updates, plan next upgrade during extended support window. This systematic approach to lifecycle management is exactly what NIS2 expects.

Supply Chain Transparency

The supply chain review represents the hardest and most important work. AVEVA reviewed over **3,000 external components** embedded in their software, assessed each for CRA readiness, and began replacing components whose suppliers won't pursue compliance. This prevents customers from inheriting hidden vulnerabilities from abandoned libraries or deprecated frameworks.

> **! Practical Example**
>
> The technology behind InTouch Access Anywhere will be retired because its supplier will not pursue CRA compliance. Instead of leaving customers exposed or uncertain, AVEVA is proactively planning secure alternatives and upgrade paths.

This supply chain discipline directly supports your NIS2 supply chain security obligations. When vendors systematically review their dependencies and ensure components meet security requirements, they're reducing your third-party risk. When vendors proactively replace non-compliant components rather than waiting for vulnerabilities to emerge, they're demonstrating the kind of risk management NIS2 expects from you. And when vendors communicate these changes clearly with migration guidance, they're enabling your compliance rather than creating surprises.

Secure-by-Design Development

The shift toward secure-by-design development practices also matters. AVEVA now incorporates secure coding practices, threat modeling, continuous vulnerability scanning, and enhanced incident response processes throughout the development lifecycle. This isn't just about passing compliance audits. It's about building products where security is intrinsic, not added later.

What This Means for You

Two regulatory deadlines feel distant until they're suddenly urgent. Organizations that start preparing now will avoid the scramble. Here's what different teams should focus on, recognizing that NIS2 is your responsibility while CRA is your vendors' responsibility, but both require your attention.

For OT Teams

- **Start with inventory.** You need to know what systems you're running, what versions, who supplies them, and when support ends. Legacy systems often lack documentation. Acquired facilities may run different technology stacks. Shadow systems built by well-meaning engineers may not appear in any official asset register. Build the inventory now.
- **Once you have inventory, assess your NIS2 scope.** Which systems fall under essential or important services? Which vendors supply those systems? Which systems are approaching end-of-support? This assessment reveals where you're most exposed and where vendor CRA compliance matters most for your operations.
- **Start vendor conversations early.** Ask suppliers about their CRA compliance plans, timelines, and migration paths. But also ask how they'll support your NIS2 requirements: How do they handle vulnerability disclosure? What's their incident response process? What visibility do they provide into supply chain components? How do they support your security monitoring needs? Vendors who answer these questions confidently are positioning you for success. Vendors who deflect are creating risk you'll need to manage.

For IT Teams

- Review your cybersecurity standards against NIS2 requirements. The directive expects risk-based measures, not checklist compliance. But industrial environments require adaptations that pure enterprise IT approaches often miss. Zero-trust architectures, identity-based access, and secure cloud connectivity need to work within operational constraints, no patching during production runs, no authentication flows that add latency to control loops, no security measures that prevent operators from responding to emergencies.
- **Build the bridge with OT now.** NIS2 compliance requires coordination between IT security and OT operations. You need shared understanding of risk priorities, agreed escalation procedures, and joint incident response capabilities. CRA gives you a forcing function for these conversations: as vendors upgrade to CRA-compliant versions, you need joint IT/OT planning for testing, deployment, and validation.

- **Prepare your procurement standards.** CRA-compliant products give you better starting security posture, but only if procurement knows what to ask for. Work with OT teams to define security requirements for industrial software purchases: support window expectations, vulnerability disclosure requirements, security documentation standards, incident response commitments. These requirements help you meet NIS2 supply chain security obligations while driving better vendor behavior.

For Leadership

- **Align CRA and NIS2 as complementary initiatives, not separate compliance projects.** NIS2 is your legal obligation. CRA is your vendors' legal obligation. But your NIS2 success depends heavily on vendor CRA compliance. Organizations that treat these as separate workstreams waste resources and miss strategic opportunities.

- Resource this properly. NIS2 compliance isn't just technical work, it requires coordination across operations, engineering, IT, procurement, legal, and risk management. CRA vendor transitions add complexity. Budget for vendor migrations, system upgrades, process development, training, and ongoing monitoring. The investment pays dividends beyond compliance: modernized systems, reduced technical debt, stronger security posture, and clearer operational visibility.

- **Make explicit decisions about legacy systems.** Every industrial organization has critical processes running on old software. You can't upgrade everything immediately. Prioritize based on NIS2 scope, operational criticality, vendor CRA commitment, and risk exposure. Some systems genuinely need modernization. Others can be isolated, monitored closely, and accepted as managed risk. The key is making conscious choices rather than drifting toward non-compliance through inaction.

- **Understand the enforcement landscape.** NIS2 includes significant penalties for non-compliance But more importantly, it includes personal liability for management bodies. Board members and executives can be held accountable for inadequate cybersecurity risk management. This isn't theoretical, regulators are actively building enforcement capabilities. Taking NIS2 seriously now is considerably cheaper than explaining failures later. Understand the enforcement landscape.

Building the Foundation for What Comes Next

The Cyber Resilience Act and NIS2 together create a new baseline for industrial cybersecurity. Vendors must build secure products. Operators must maintain secure operations. Neither obligation is optional, and neither can succeed without the other.

The organizations that view these regulations as pure compliance burdens will do the minimum required and miss the larger opportunity. The organizations that view them as catalysts for organizational maturity will use them to accelerate conversations they should have been having anyway.

Key Questions to Address

- How do we manage technical debt systematically?
- How do we ensure IT and OT collaborate effectively?
- How do we balance innovation with operational stability?
- How do we build digital foundations that support the next decade of industrial operations?

These questions matter whether or not CRA and NIS2 exist. The regulations simply make them urgent, and provide external justification for investments that were already needed. That urgency can be productive if you use it strategically.

Start with clarity about responsibility. Your vendors are accountable for CRA compliance. You can't do their work for them, and you shouldn't accept products that don't meet CRA requirements. But you are accountable for NIS2 compliance. You can't delegate that responsibility to vendors, and you can't assume that CRA-compliant products automatically satisfy your NIS2 obligations.

For NIS2

Assess your scope, inventory your systems, review your risk management processes, and strengthen coordination between IT and OT.

For CRA

Engage with vendors about their compliance plans, understand migration timelines, and prepare for system upgrades.

And for both: recognize that these aren't separate compliance projects, they're two sides of the same imperative to secure industrial operations for the next decade.

What's your first move?

The work starts now.

Factory Software

Industrial Software for Connected Operations

www.factorysoftware.com

© 2026 Factory Software. All rights reserved.

This whitepaper is provided for informational purposes only. While we strive to keep the information up to date and correct, we make no representations or warranties of any kind about the completeness, accuracy, reliability, or suitability of the information contained herein. Please consult with us, legal and other cybersecurity professionals for advice specific to your situation.