Rethinking IoT Strategy in the Era of EU Regulation

Whitepaper

NIS2-Friendly IoT for Device Manufacturers

Process driven, backbone supported, value propositions within the NIS2 context

LYXION
INDUSTRIAL IOT PORTFOLIO MANAGEMENT

CUMULOCITY

NIS2-Friendly IoT for Device Manufacturers

Designing Products for Regulated Operational Environments

Scope and Context: Beyond the Checklists

When preparing this whitepaper, it became apparent that a significant amount has already been written about the NIS2 Directive itself. Most publications focus heavily on regulatory interpretation, legal obligations, or prescriptive technical security controls.

But far less attention has been given to what it means for technologies, device manufacturers, and distributors to actually be "**NIS2-friendly**".

Much of the existing material emphasizes the usual suspects:

- Governance and management accountability
- Cybersecurity risk management measures
- Incident reporting
- Supply chain security
- Business continuity and resilience

While essential, these aspects are already well documented and remain largely focused on the NIS2 entities themselves. Although we do recognize that IT, OT, and IoT require different approaches, (With IoT often missing) this whitepaper does not aim to explore those distinctions in detail.

Instead, together with the Cumulocity team, we chose to dedicate a specific section to device manufacturers and their role in the NIS2 chain.

So

Accordingly, this whitepaper takes a more practical perspective. It focuses on a central question:

How can device manufacturers design products and supporting documentation so they can be considered NIS2-friendly?

Part 1: The Regulatory Shift

1. Why NIS2 Changes the Device Conversation

The introduction of the NIS2 Directive is changing how buyers evaluate connected devices and solutions. Especially for organizations operating in critical infrastructure, healthcare, manufacturing, energy, or transport, the question is no longer simply whether a device is secure in isolation. The much question is now whether that device can integrate effortlessly into their ongoing governance, risk, and audit processes.

This shift towards NIS2 compliance affects procurement, deployment, and lifecycle management, while also increasing the need for stronger organizational alignment and clearer ownership. Furthermore, when it comes to IoT hardware, regulated customers now require immediate clarity on how a device is updated, who is responsible for monitoring it, which logs are available, how incidents are triaged, and how the device's state can be evidenced to an auditor over a ten-year lifespan. A device that cannot support these expectations becomes harder to approve, harder to manage, and more likely to be viewed as an operational liability during an audit.

2. Why CRA Is Necessary but Not Sufficient

The Cyber Resilience Act (CRA) provides a vital baseline for digital product security. It pushes manufacturers toward secure-by-design development, vulnerability handling, and lifecycle support. This foundation ensures the hardware is fundamentally safe when it leaves the factory, and these requirements will become the regulatory framework manufacturers must follow to obtain CE conformity for digital products.

However, meeting CRA requirements alone does not explain how to operate those devices within a highly regulated facility. CRA secures the *product*, but NIS2 governs the *operation*. A secure-by-design certification does not inherently create fleet visibility, ongoing risk management workflows, or the continuous audit verification required by NIS2. Therefore, while CRA is a necessary starting point, it is not sufficient to clear the procurement hurdles of a NIS2-regulated buyer.

3. From Product Security to Operational Governance

To satisfy NIS2, regulated organizations must manage their deployments within strict governance frameworks. They cannot simply install a CRA-certified device and forget about it. They must be able to confidently answer auditors on an ongoing basis:

- Who owns the device and its associated processes?
- How are risk decisions regarding this device made and documented?
- How are incidents detected and escalated?
- How are vulnerabilities actively handled?
- How are external dependencies tracked?
- How is execution evidence retained for audit and review?

These are rigorous governance challenges, not just technical hurdles. A device that is highly secure but opaque "black box", acts as an operational liability because it forces the end-user to figure out how to answer these questions entirely on their own.

This is where the concept of "NIS2-friendly" becomes a powerful differentiator for device manufacturers. NIS2 friendly should not be confused with legal NIS2 compliance, which applies directly to the essential or important organizations deploying the technology.

Rather, NIS2-friendly design is an operational philosophy. It is the manufacturer's direct response to the governance burden outlined above. It describes how manufacturers can design products and supporting materials, so they natively support the end-user's operational governance and lifecycle management.

A NIS2-friendly device arrives with a rich operational context surrounding its deployment, maintenance, and end-of-life.

This includes clear network architecture guidance, update mechanisms, support boundaries, and explicit documentation of what the device can and cannot do on its own.

By translating a product’s technical characteristics into these operational consequences, device manufacturers can deliver more than just hardware; they deliver a transparent operational blueprint that directly answers the governance questions their buyers face.

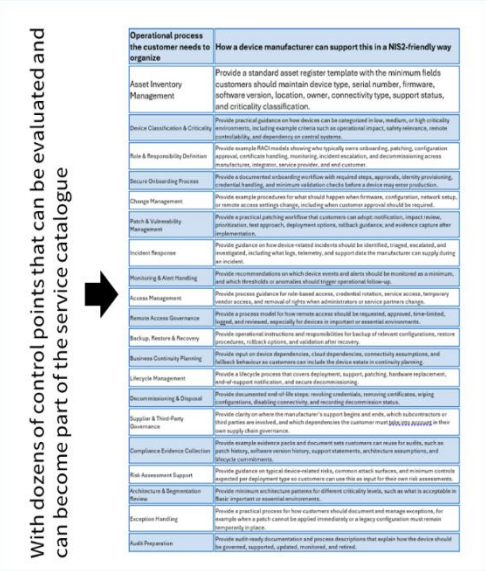
Part 2: What Customers Need in Practice

4. The Information Buyers Actually Need

Traditional technical documentation serves engineers perfectly, but it leaves procurement, compliance, and SOC teams starved for governance context.

A buyer in a regulated environment needs explicit clarity on where the device is intended to operate, what network conditions it expects, its default security posture, how firmware updates are delivered, what logging is available, external dependencies, and support boundaries.

The most valuable documentation translates raw technical features into operational realities. For example, if a device supports encrypted communication, that is useful. But if intrusion detection still depends on external monitoring, the customer absolutely needs to know that too.



In Practice: Risk Acceptance and Compensating Controls

Under NIS2, organizations cannot simply fix vulnerabilities as they arise; they must formally document decisions regarding risk acceptance, mitigation, and escalation in their risk registers and supplier assessments.

How does a device manufacturer help? By providing operational context that extends far beyond a standard spec sheet.

Transparent documentation of product limitations is actually a massive asset.

For example, if a manufacturer clearly states a constraint, such as limited on-device logging capacity or a lack of automated patching, the customer isn't caught off guard during a security audit. Instead, the customer uses that transparent baseline to implement appropriate *compensating controls*, such as placing the device behind a specific firewall-level or adding intrusion monitoring. Decisions become significantly easier for an end-user to justify when the manufacturer provides this honest operational context, particularly when the device's actual state is verifiable through connected dashboards rather than hidden in static documents.

5. When Lifecycle Management Hits Reality

A device manufacturer can only be truly NIS2-friendly if it understands the operational reality of the NIS2-regulated customer. In practice, organizations are rarely just managing one isolated connected product, but more likely a horizontal and vertically integrated landscape of IoT solutions from different manufacturers, integrators, service partners, and internal teams.

What seems manageable at product level quickly becomes far more complex in the customer's real operating environment.

Patching, monitoring, logging, asset tracking, and secure decommissioning are straightforward enough when applied to a single device, a single solution. The real challenge begins when these activities must be executed consistently across large fleets, over many years, and across dozens of different solutions.

For **NIS2-regulated customers**, this creates **a practical governance challenge**. Each solution comes with its own tooling, documentation style, update logic, and support model. Documentation alone is therefore rarely enough. Firmware tracking spreadsheets become outdated, log collection becomes inconsistent, patch evidence fragments across systems, and responsibilities can blur between manufacturers, integrators, and operators.

This also leads to a reverse-engineering problem. Customers and system integrators end up translating PDF guidance into manual workarounds: creating their own firmware trackers, writing scripts for log extraction, combining dashboards, and assembling audit evidence by hand. The friction is not necessarily caused by poor documentation, but by the gap between documented expectations and operational reality.

That is why Lyxion believes real value emerges when process guidance is supported by a dynamic, technical backbone that can bundle isolated or siloed IoT Solutions under a single security umbrella. (More on that later)

But it is evident that, when documentation and tooling go hand in hand, lifecycle tasks become more scalable, evidence collection more reliable, and compliance far easier to operationalize across a diverse solution landscape.

As a consequence, device manufacturers should not stop at documenting NIS2-friendly processes. They can take a real step into the world of their customers by integrating those processes into a technical backbone that acts as a demonstrator platform. This gives customers, integrators, and service partners a practical environment to see how lifecycle management, traceability, monitoring, and evidence collection can work in reality.

Rather than forcing them to reverse-engineer documentation into their own ad hoc operating model.

Part 3: The Execution Layer

6. The Role of the Technical Backbone for NIS2 entities

To reduce the friction for implementing standalone compliance frameworks, Lyxion advises organizations to adopt a technical management backbone: an execution layer that helps turn static compliance guidance into live operational practice.

This backbone connects device state, lifecycle events, access control, firmware history, and telemetry into a structure that can support governance, traceability, and evidence collection.

Rather than leaving each customer or system integrator to build/invent custom processes from scratch, an enterprise-grade IoT platform can serve as a controling backbone, providing a repeatable foundation for managing device fleets in a scalable and audit-supportable way. It helps operationalize patching, visibility, logging, access control, and lifecycle tracking without forcing customers to recreate that logic themselves through fragmented tooling.

While customers remain free to choose, what we call, “a TIER1 platform” that best fits their environment, Lyxion strongly recommends benchmarking and evaluating requirements against top-tier IoT solution aggregators such as Cumulocity.

In our comparative assessment, Cumulocity distinguishes itself through strong compliance-supporting capabilities, security-by-design principles, interoperability-oriented architecture, true multi-tenancy, hybrid deployment flexibility, and API-driven integration.

The value of comparing against the best is not to force a decision, but to ensure that no critical requirement is overlooked in the best-practice foundation fo a scalable and secure IoT architecture.

7. Translating the Blueprint into Executable Workflows

The true value of an enterprise-grade platform like Cumulocity lies in how it takes the manufacturer's NIS2-friendly blueprint and executes it in an operational reality.

When documentation and tooling go hand in hand, the platform serves as an engine that translates the static rules of governance into automated workflows. This platform-driven approach drastically improves how compliance is managed on the ground across the three most critical operational domains:

- **Automated Traceability & Patching:** Instead of hoping end-users follow a written manual, Cumulocity can natively execute over-the-air (OTA) update campaigns. It logs configuration changes, helping translate the manufacturer's theoretical patch policy into automated, time-stamped proof for auditors.
- **Audit-Ready Asset Visibility:** Manual spreadsheets often become outdated the moment they are saved. Cumulocity replaces them with a real-time digital twin of deployed devices, offering an accurate inventory of connection states, health metrics, and firmware versions.
- **Post-Incident Evidence:** During a security anomaly, manual log retrieval is often too slow. Cumulocity's continuous telemetry tracking provides structured evidence of device behavior, allowing incident response teams to act more decisively.

While operational documentation provides the essential compliance blueprint, an IoT platform acts as the engine that turns that theory into verifiable execution. However, to truly eliminate deployment friction, this technical connection should not be left for the customer to build from scratch, it yields the greatest commercial advantage when it is pre-wired into the device before it ever reaches the field.

8. What Ecosystem Pre-Integration Delivers

This "pre-wiring" is achieved through ecosystem pre-integration. When device manufacturers align their hardware with platforms like Cumulocity during the design phase, they make the technical backbone immediately accessible to the market.

Because the data models, logging taxonomy, and update mechanisms are already mapped to the platform, buyers no longer have to imagine how governance will work in practice. Nor do they have to fund costly IT projects to build the reporting integrations themselves.

For system integrators, this significantly improves the delivery model. Instead of spending weeks writing custom scripts to translate a new router's telemetry into an audit dashboard, integrators inherit an operational model that is already aligned with NIS2 principles. The heavy lifting of translating the manufacturer's PDF manual into actionable software has already been done.

This pre-wired connectivity acts as a powerful implementation accelerator. Procurement and security teams are presented with a clearer, more defensible compliance path, drastically shortening the journey from technical validation to operational deployment.

Part 4: Commercial Implications

9. Immediate Commercial Value: Removing Procurement Friction

The commercial value of being NIS2-friendly is immediate, but it is strongest when the operational story is complete. Manufacturers that provide structured documentation, lifecycle transparency, and ecosystem alignment are fundamentally easier to trust. They reduce the workload for security, compliance, and procurement stakeholders, lowering the risk that a hardware deal will stall due to a lack of operational proof.

Furthermore, device manufacturers rarely sell directly to the end-user; distribution partners, value-added resellers, and system integrators often act as intermediaries. These channel partners also benefit immensely when they can deliver an audit-ready solution quickly, rather than building compliance infrastructure from scratch to satisfy their clients.

In regulated markets, the ability for manufacturers or resellers to show operational governance via f.e. Cumulocity pre-integration, can become a sales accelerator.

This then also serves as a sharp commercial differentiator that separates strategic technology partners from commodity hardware vendors.

10. Long-Term Value: The Shift to Lifecycle Business Models

Beyond immediate sales enablement, cybersecurity regulation is encouraging the market to move away from one-time product delivery and toward continuous, lifecycle-based support.

This shift invites manufacturers to reconsider traditional, transactional business models.

This does not mean every hardware manufacturer must magically transform into a software or a consulting company. However, it does mean manufacturers should consider how they will monetize and support updates, vulnerability handling, and operational transparency over the 5- to 10-year lifespan of a device.

Lifecycle services, such as premium monitoring tiers, automated compliance reporting, and managed OTA updates, become highly credible when anchored in a managed technical backbone.

By leveraging Cumulocity as an execution engine, manufacturers can seamlessly evolve their business models. They can transition from merely shipping devices to securing recurring revenue streams based on supporting long-term operational outcomes, all without having to build the underlying platform infrastructure themselves.

11. Final Perspective: Designing for Defensible Operations

NIS2 is changing what customers expect from connected devices. Secure hardware remains essential, but it is rarely enough on its own. Regulated buyers need devices that can be governed, monitored, updated, and audited as part of a larger, highly scrutinized operational system.

This is why NIS2-friendly design matters. It provides an operational blueprint, giving manufacturers a way to support regulated customers without turning themselves into compliance consultants.

And this is where a technical backbone can serve as a strategic accelerator: it turns documentation into execution, and execution into verifiable evidence with a predefined governance framework.

The winning approach in the channel is educational clarity combined with operational execution: explain the governance need and then provide the technical means to satisfy it. Transparent documentation, enhanced by ecosystem pre-integration, is what empowers device manufacturers to become credible, indispensable partners in critical infrastructure.

Lyxion has more than 10 years of experience with Cumulocity, during which we have seen it evolve from one of the leading IoT platforms into one of the few capable of supporting full NIS2 compliance. At the same time, we want to stress that, in our view, NIS2 compliance is 80% about processes and documentation, and 20% about technology.

That said, the right 20% in technology can make the remaining 80% significantly easier to implement, manage, and maintain.

Lyxion | Bridging compliance, technology, and operations in IoT, IIoT, and OT

Lyxion helps organizations design and manage connected environments that are secure, compliant, and operationally sustainable. By combining advisory, governance, compliance, and ecosystem expertise, we support clients in turning complexity into practical progress.

LYXION
INDUSTRIAL IOT PORTFOLIO MANAGEMENT

CUMULOCITY