RX-OS

COGNITIVE SECURITY

NIS2 Compliance Guide for Belgian Critical Infrastructure

2026

A practical guide to achieving NIS2 compliance

with on-premise cognitive security.

For CISOs, IT Managers, and Compliance Officers

at hospitals, factories, and essential entities.

By Sator Tech | Aalst 9300, Belgium

info@rx-os.eu | rx-os.eu

EXECUTIVE SUMMARY

What NIS2 means for your organization

The NIS2 Directive (EU 2022/2555) is the most significant cybersecurity regulation ever enacted in Europe. It applies to all essential entities including hospitals, energy providers, water utilities, transport operators, and manufacturing companies with more than 50 employees.

In Belgium, the Centre for Cybersecurity Belgium (CCB) has transposed NIS2 into national law. The compliance deadline for essential entities is **18 April 2026**. Organizations that fail to comply face penalties of up to EUR 10 million or 2% of global annual turnover.

The challenge is clear:

- NIS2 requires continuous risk management, not annual audits
- Incident reporting must happen within 24 hours of detection
- Supply chain security must cover every connected device
- Evidence must be tamper-proof and auditable
- Management is personally liable for compliance failures

Most organizations attempt compliance with traditional IT security tools designed for corporate networks. These tools miss the operational technology (OT) and IoT devices that NIS2 explicitly requires you to protect: medical equipment, building automation systems, industrial controllers, cameras, and access control systems.

RX-OS takes a fundamentally different approach. It is a cognitive security system that runs entirely on-premise, discovers every device on the network regardless of protocol, and produces cryptographically verifiable compliance evidence.

This guide explains the 10 requirements of NIS2 Article 21, how RX-OS addresses each one, and why on-premise cognitive security is the only approach that satisfies both the letter and spirit of the directive.

NIS2 ARTICLE 21

The 10 requirements, explained

Article 21 of the NIS2 Directive mandates that essential and important entities implement cybersecurity risk-management measures. Below, each requirement is explained in practical terms with how RX-OS provides coverage.

Art. 21(2)(a) — Risk Management

Policies on risk analysis and information system security.

RX-OS coverage: RX-OS performs continuous risk assessment using a causal reasoning engine based on Pearl do-calculus. Risk is quantified in EUR, not abstract scores. The system predicts incidents before they happen by modeling causal relationships between network events.

Art. 21(2)(b) — Incident Handling

Procedures for detecting, reporting, and responding to incidents.

RX-OS coverage: Automated incident detection with 24-hour early warning capability. The system generates incident timelines, classifies severity, and produces the three-stage reporting required by NIS2: early warning (24h), notification (72h), final report (1 month).

Art. 21(2)(c) — Business Continuity

Business continuity and crisis management.

RX-OS coverage: Configurable kill switch with automatic threat containment. The cognitive firewall can isolate compromised devices at kernel level within milliseconds while maintaining operational continuity for unaffected systems.

Art. 21(2)(d) — Supply Chain Security

Security of the supply chain and supplier relationships.

RX-OS coverage: Every device on the network is autonomously discovered, identified by vendor and firmware version, and continuously monitored. Unauthorized devices are detected within seconds. No cooperation from the device is required.

Art. 21(2)(e) — Network Security

Security in network and information systems acquisition, development, and maintenance.

RX-OS coverage: eBPF programs operate at the kernel level for wire-speed packet inspection. The cognitive firewall writes its own rules in real-time based on threat analysis. Protocol-aware deep packet inspection covers 30+ industrial and IT protocols.

Art. 21(2)(f) — Access Control

Policies and procedures for evaluating effectiveness of measures.

RX-OS coverage: JWT token-based authentication with role-based access control (admin, operator, viewer). Account lockout protection, session management, and complete audit trail of every user action.

Art. 21(2)(g) — Cryptography

Policies and procedures regarding the use of cryptography and encryption.

RX-OS coverage: Mutual TLS 1.2+ for all communications. Self-signed certificate generation and management. Hash-chained audit trail using SHA-256. Password storage with PBKDF2 (100,000 iterations). All evidence is cryptographically sealed.

Art. 21(2)(h) — Human Resources Security

Human resources security and cybersecurity training.

RX-OS coverage: User management with enforced role separation. Complete activity logging per user including timestamp, action, target, and source IP. Every administrative action is recorded in the immutable audit trail.

Art. 21(2)(i) — Asset Management

Asset management including hardware and software inventory.

RX-OS coverage: Autonomous device discovery via ARP scanning, port probing, and protocol fingerprinting. Devices are classified by vendor, type, firmware, protocols, and risk score. Cognitive possession creates digital twins for continuous monitoring.

Art. 21(2)(j) — Vulnerability Management

Vulnerability handling and disclosure.

RX-OS coverage: Continuous port scanning and service detection. AR(2) autoregressive anomaly detection per sensor. CUSUM change-point analysis for regime shift detection. Isolation Forest for multivariate anomaly correlation.

DATA SOVEREIGNTY

Why on-premise matters

NIS2 and GDPR create a regulatory environment where the location and control of security data is as important as the security measures themselves. Cloud-based security platforms introduce risks that directly conflict with compliance objectives.

The cloud problem

- Device telemetry leaves your building and enters third-party infrastructure
- Audit trails are stored on servers you do not control
- Vendor access to your network topology creates supply chain risk
- Data processing agreements add legal complexity
- Service availability depends on external internet connectivity

The RX-OS approach

RX-OS runs entirely on hardware you own and control. The edge appliance sits on your network. The brain processes data on your server. No telemetry leaves your building. No cloud subscription. No external dependency.

For Belgian hospitals handling patient data, this is not a preference. It is a legal necessity. GDPR Article 28 requires data controllers to ensure processors provide sufficient guarantees. With RX-OS, you are the processor. The data stays in your building, under your control, subject to Belgian law.

ARCHITECTURE

The RX-OS approach

Edge Appliance + Brain

RX-OS uses a split architecture. A physical edge appliance is deployed at the customer site. It connects to the local network and immediately begins discovering devices. The brain, running on a separate server, performs cognitive reasoning, causal analysis, and compliance reporting.

Communication between the edge and brain uses mutual TLS over MQTT. If the connection is interrupted, the edge continues operating independently and buffers data until connectivity is restored.

Cognitive possession

Unlike passive monitoring tools that observe network traffic, RX-OS actively identifies and profiles every device. It reads registers from PLCs via Modbus, queries switches via SNMP, probes cameras via ONVIF, and fingerprints operating systems from packet signatures. This is cognitive possession: the system does not just see a device. It understands what the device is, what it does, and what it should be doing.

Hash-chained audit trail

Every security event is recorded in a hash-chained audit log. Each entry contains a SHA-256 hash computed from the entry content and the hash of the previous entry. The chain starts from a GENESIS block. Any attempt to modify, insert, or delete an entry breaks the chain and is immediately detectable.

This provides cryptographic proof of compliance. An auditor can verify the integrity of the entire audit trail by recomputing hashes from the beginning. No traditional log system offers this level of tamper resistance.

RISK QUANTIFICATION

Risk in euros, not scores

Abstract risk scores (high/medium/low) do not help a board make investment decisions. RX-OS quantifies cyber risk in EUR using a methodology aligned with the FAIR (Factor Analysis of Information Risk) framework.

How it works

- Each discovered device is assigned a replacement cost and operational impact value
- Threat probability is estimated from device exposure, patch status, and protocol security
- Annual loss expectancy = threat frequency x impact magnitude
- The dashboard shows a single EUR figure that updates as the network changes

When a new unmanaged device appears on the network, the risk figure increases. When a device is brought under cognitive possession and its firmware is verified, the risk figure decreases. This creates a clear incentive loop: the more you monitor, the lower your quantified risk.

DEPLOYMENT

Three steps. Fifteen minutes.

Step 1: Connect the edge appliance

Plug the RX-OS edge appliance into any network port. No agents to install on endpoints. No configuration changes to switches or firewalls. No disruption to operations. One ethernet cable.

Step 2: Discovery begins automatically

Within minutes, the edge appliance maps every device on the network. IT equipment, OT controllers, medical devices, cameras, access control systems, building automation. Each device is identified by vendor, model, firmware, and protocols.

Step 3: Brain reasons and reports

The RX-OS brain analyzes the discovered environment. Causal reasoning identifies risk relationships. Anomaly detection baselines normal behavior. The NIS2 compliance score is calculated. Reports are generated. The system is operational.

COMPARISON

How RX-OS compares

Capability	Traditional Tools	Cloud Platforms	RX-OS
Detection method	Scheduled scans	Passive traffic	**Kernel + AI fused**
OT protocol support	None	Classify only	**30+ native protocols**
Data location	Varies	US/Israel cloud	**On-premise only**
Audit trail	Log files	Vendor-managed	**Hash-chained**
AI reasoning	None	Risk scoring	**Causal engine**
Digital twins	None	None	**Cognitive twins**
Kernel integration	None	None	**eBPF native**
NIS2 evidence	Reports only	Dashboards	**Cryptographic proof**
Deployment	Weeks	Days	**15 minutes**

CYBERFUNDAMENTALS

Belgium's path to NIS2

The Centre for Cybersecurity Belgium (CCB) has created the CyberFundamentals Framework as the practical translation of NIS2 into measurable controls.

Four levels

- **Small** — Minimal controls, self-assessment. For micro-organizations.
- **Basic** — 34 controls, independent verification. Covers 82% of attacks. Minimum for NIS2 suppliers.
- **Important** — 99+ controls, independent verification. Covers 94% of attacks.
- **Essential** — Full control set, formal certification. Required for hospitals and critical infrastructure.

How to start

- Register at atwork.safeonweb.be for the free self-assessment toolbox
- Implement the 34 Basic controls as a minimum
- Engage an accredited Conformity Assessment Body for verification
- Consider ISO 27001 certification for international credibility

VLAIO (Flemish Agency for Innovation and Enterprise) provides subsidies covering 35% of cybersecurity consultancy costs for SMEs. This can significantly reduce the cost of achieving CyberFundamentals certification.

ABOUT

Sator Tech

RX-OS is designed, built, and maintained by Sator Tech in Aalst, Belgium. The system is the result of deep engineering in kernel-level security, artificial intelligence, and industrial protocol analysis.

Key facts

- **49 live services** running in production
- **114,942 lines** of production code
- **30+ industrial protocols** supported natively
- **2 patents pending** on novel security architecture
- **100% on-premise** — no cloud dependency
- **Built on RXL** — a purpose-built systems language for cognitive devices

Contact

Email	info@rx-os.eu
Website	rx-os.eu
Location	Aalst 9300, Belgium
Response time	Within 24 hours