framatome cybersecurity

Complying with European Network and Information Security (NIS2) in OT environments

Cybersecurity requirements for critical infrastructure operators

Introduction

NIS2 (Directive (EU) 2022/2555) is the European Union's updated cybersecurity framework aimed at achieving a high common level of cybersecurity and resilience across Member States.

Building on the original NIS Directive, NIS2 broadens its scope by covering a larger number of sectors and entities, including both Essential and Important Entities. It introduces enhanced cybersecurity risk management, incident reporting, supply chain security and governance requirements, while strengthening management accountability and regulatory oversight.

The OT Dimension of NIS2

Applying NIS2 cybersecurity requirements in industrial and operational technology (OT) environments requires more than simply translating IT security practices into the plant.

Industrial systems operate under constraints that differ fundamentally from IT. Safety-certified controllers, legacy equipment and production-critical systems often cannot support endpoint protection, frequent patching or standard hardening measures without impacting safety, reliability or operational continuity.

The challenge is therefore not to apply every security measure identically, but to demonstrate that NIS2 cybersecurity objectives are effectively achieved in the OT context. This requires a risk-based approach that identifies applicable requirements, evaluates technical and operational constraints, implements compensating controls, and documents decisions in a manner that is transparent, auditable and defensible.

The objective is not compliance at the expense of operations, but resilient and demonstrable cybersecurity that supports safety, availability and business continuity.



With its unique positioning as an expert in both industrial systems and cybersecurity, Framatome Cybersecurity allows Essential and Important Entities throughout EU Member States to address NIS2 requirements and demonstrate a robust and defensible cybersecurity posture without compromising safety, availability, or business performance.

Your performance
is **our** everyday **commitment**

How we help

In industrial environments, NIS2 compliance is not about applying security controls indiscriminately. It is about demonstrating that cyber risks for critical operations are effectively managed through measures that remain compatible with safety, availability and business performance.

NIS2 essential measure	Operational & business objective	Framatome Cybersecurity support
Risk analysis & information system security policies	Understand and prioritize cyber risks affecting critical operations, industrial assets and business services, and provide management with a defensible basis for security decisions.	› Governance & Organization › Vulnerability Operations Center › Asset Management › Cyber Program Management
Incident handling	Detect, respond and contain cyber incident before they impact safety, production, regulatory obligations or customer commitments.	› Performance & Cyber monitoring › Vulnerability Operations Center › Cyber Program Management
Business continuity, backup, disaster recovery & crisis management	Maintain or rapidly restore critical operations following a cyber incident while minimizing operational, financial and reputational impacts.	› Cyber Program Management › Crisis Management & Exercise › Resilience Assessment Services
Supply-chain security	Secure dependencies — manage cybersecurity risks arising from suppliers, service providers, products and critical third-party relationships.	› Governance & Organization services › Cyber Program Management › Supplier Security Assessment Support
Security in acquisition, development & maintenance, including vulnerability handling	Ensure systems remain secure throughout their lifecycle while preserving safety, reliability and maintainability of industrial operations.	› Architecture design › Hardening services › Vulnerability Operations Center › Performance & Cyber monitoring
Assessing the effectiveness of cybersecurity risk-management measures	Demonstrate that cybersecurity measures effectively manage risk and provide auditable evidence to management, customers and regulators.	› Organizational & Technical audits › Maturity Assessments › Compliance & Readiness Reviews

About Us

Framatome Cybersecurity: Protecting what powers the world

A robust defense-in-depth approach at overall and system level during the complete lifecycle of a critical infrastructure facilities:

- Dedicated team of 270+ engineers specialized in industrial cybersecurity for critical industrial systems
- Supporting 1000+ customers operating critical infrastructures worldwide
- Experts on regulation and certification:
  ISO, IEC, NIST, UK NISR, French LPM, US NRC, NIS2, NERC CIP, RCC-E

Contact: cyber-services@framatome.com
Website: Cybersecurity Solutions Portfolio

framatome cybersecurity

The data and information contained herein are provided solely for illustration and informational purposes and create no legal obligations by Framatome. None of the information or data is intended by Framatome to be a representation or a warranty of any kind, expressed or implied, and Framatome assumes no responsibility or liability for the use of or reliance on any information or data disclosed in this document.
All rights reserved. © 2026 Framatome. All rights reserved.