NOZOMI NETWORKS

COMPLIANCE MAPPING GUIDE

European Network and Information Security (NIS2) Compliance with Nozomi Networks' Solution

1. Introduction

Updates to the latest iteration of the NIS2 Directive to coordinate cybersecurity across the European Union specify new terms and mandates for Member States. The guidance tasks leaders with applying cybersecurity considerations and requirements to entities that serve a large part of the population and are considered vital to the economy, based on services provided and size of operations.

While the original Directive came into effect in May 2018, EU Member States are directed to adopt provisions included in the updated Directive by October 2024 and produce associated details of how they plan to comply. Updates to the Directive expand its scope to include new critical sectors, and additional considerations for determining "essential" vs. "important" entities.

NIS2 incorporates a two-phased incident reporting structure. Regardless of proactive or reactive supervision, the legislation mandates any significant incident to be reported within 24 hours of onset, adding details within 72 hours. More detailed reporting is required as a follow-on measure one month after the onset of a significant incident. This structure is an attempt to swiftly capture immediate details to prevent widespread impacts from similar attacks, and to provide in-depth analysis after the fact for security researchers and future resilience planning.

A significant cybersecurity incident is defined as an incident that either has cause or is capable of causing severe operational disruption of the services or financial loss for the entity concerned, and/or has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage. Entities are further expected to indicate whether they suspect the significant incident is the result of unlawful or malicious activity, and whether the incident might have transnational impacts.

NIS2 calls out the broad spectrum of resources available to entities to carry out cybersecurity considerations and requirements, noting "the supervisory and enforcement regimes for those two categories of entities should be differentiated to ensure a fair balance between risk-based requirements and obligations on the one hand, and the administrative burden stemming from the supervision of compliance on the other." Compliance is mandatory, and failure to do so could still result in significant fines. Fines for non-compliance could equal €10 million or 2% of global turnover for Essential Entities, and €7 million or 1.4% of global turnover for Important Entities.

2. NIS Directive Scope

Essential Entities replaces the previous category of operators of essential services and generally encompasses organizations with ~250 or more employees, annual turnover of €50 million or balance sheet of €43 million. Important Entities are significant sectors whose disruption would not necessarily cause serious societal or economic consequences, with ~50 employees, annual turnover of €10 million or balance sheet of €10 million. The legislation hopes to ramp up cyber defences without attempting to 'boil the ocean.'

Important Entities:

- Postal and courier services
- Waste management
- Manufacture, production, and distribution of chemicals
- Food production, processing, and distribution
- Manufacture of medical devices, electronic products, and transport
- Digital providers
- Research

Essential Entities:

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Wastewater
- Digital infrastructure
- ICT-service management
- Public administration entities (excluding the judiciary, parliament, and central banks)

3. NIS Directive Compliance

Given that NIS is a principle-based approach, how does an organisation demonstrate 'compliance' with the NIS Directive?

Article 7 mandates each Member State in the EU to adopt a national security strategy with the following strategic objectives in mind and in scope:

- Objectives and priorities of the Member State's cybersecurity strategy
- A governance framework to achieve stated objectives and priorities
- A governance framework clarifying roles and responsibilities for Member State stakeholders, established points of contact, and computer security incident response teams (CSIRTs)
- A mechanism to identify relevant assets and Member State risk assessments
- An identification of the measures ensuring preparedness, response, and recovery planning to include public-private cooperation
- A list of the authorities and stakeholders involved in the implementation of the national cybersecurity strategy established by and for the Member State

Article 7 stipulates additional policies each Member State shall incorporate into their strategies, including ICT supply chain considerations, guidance for small and medium-sized enterprises, vulnerability management, internet security, requirements for adopting certain technologies and information sharing tools, training and education, and plans to enhance the general level of cybersecurity awareness for citizens in the general population.

Member States are required to adopt a national strategy and carry out regular risk assessments to identify entities that are considered essential or important to society and the economy. One tool to aid Member States is the Cyber Assessment Framework. The Cyber Assessment Framework offers a systematic method for assessing the extent to which entities are achieving the outcomes specified by the NIS principles. It can be used by oversight bodies when assessing entities, or by entities and their stakeholders as a self-assessment tool.

Risk management in Article 21 is three-pronged, tackling technical, operational, and organizational approaches to the security of network and information systems entities

rely on for the provision of goods and services. The legislation directs entities to assess the proportionality of risk management activities, considering their degree of exposure to risks, size, likelihood of incidents and their severity, and the societal and economic impacts stemming from potential incidents.

As a baseline, NIS2 recommends including the following measures in each risk management program at the entity/organisation level:

- Policies on risk analysis and information system security
- Incident handling
- Business continuity, such as backup management and disaster recovery, and crisis management
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
- Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- Basic cyber hygiene practices and cybersecurity training
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption
- Human resources security, access control policies, and asset management
- The use of multi-factor authentication or continuous authentication solutions

3.1. Comparable U.S. Cybersecurity Standards

- North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Cybersecurity reliability standards, approved by the Federal Energy Regulatory Commission (FERC)
- CISA's Cross-Sector Cybersecurity Performance Goals (Common Baseline Controls and sector-specific controls and goals)
- Department of Energy (DOE)'s Cybersecurity Capabilities Maturity Model (C2M2)
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®)

4. How the Nozomi Networks Solution Supports the NIS Directive

NIS2 is only one part of a broader 5-point plan the EU is enacting to address cybersecurity. The European Commission will continue to expand on technical and methodological requirements related to the NIS2 Directive. The Nozomi Networks platform allows Essential and Important Entities throughout EU Member States to anticipate, diagnose, and respond to cybersecurity incident and process anomalies across critical operational technology and IoT networks.

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Our platform delivers information that enables an intelligent and targeted approach to cybersecurity within ICS environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

Nozomi Networks provides real-time network intelligence, monitoring and AI-powered threat detection. This enables a proactive approach to risk management and ultimate reduction. It also provides real-time alerts to threats and anomalies within an industrial control network. Our solution includes a flexible and intuitive interface for reporting and operational oversight, equipping entities to develop a level of cybersecurity maturity that aligns with and demonstrates compliance with the NIS2 Directive.

4.1. Risk Management and Reporting Obligations

While all entities are subject to these seven broad security requirements, NIS2 requires Essential Entities to have proactive supervision and oversight on requirements, while Important Entities are subject to reactive supervision if/when a reported incident is significant and triggers supervision. The table below details how Nozomi Networks' solutions support each security objective for OT/ICS networks.

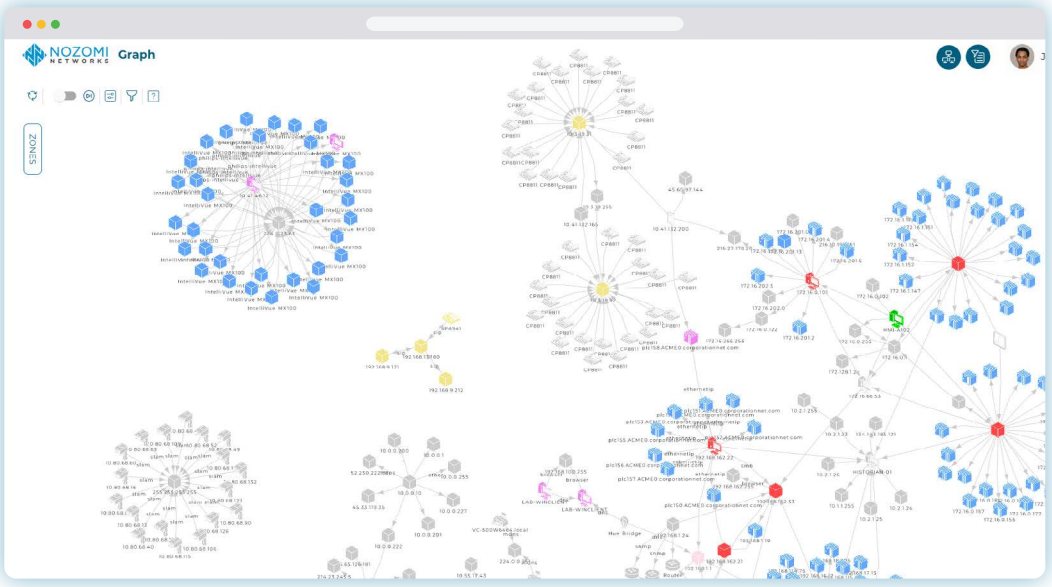
Requirement	Security Objectives	Nozomi Networks Support for OT/ICS Networks
Policies on risk analysis and information systems security policies	The operator establishes a mapping of its ecosystem, including internal and external stakeholders, including but not limited to suppliers, in particular those with access to or managing operator's critical assets.	COMPLETE
	The operator establishes and updates a policy and procedures for performing information system security assessments and audits of critical assets and Critical Information Systems (CIS), taking into account the regularly updated risks analysis.	COMPLETE
	The operator conducts and regularly updates a risk analysis, identifying its CIS underpinning the provision of the essential services of OES and identifies the main risks to these CIS.	COMPLETE
	Building upon the risks analysis, the operator establishes, maintains up-to-date and implements an information system security policy (ISSP) approved by senior management, guaranteeing high level endorsement of the policy.	PARTIAL
Incident handling: any actions and procedures aiming to prevent, detect, analyse, and contain or respond to and recover from an incident	The operator creates and keeps up-to-date and implements a procedure for handling, response to and analyses of incidents that affect the functioning or the security of its CIS, in accordance with its ISSP.	PARTIAL
	There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential services in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.	PARTIAL
	The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the delivery of essential services, even when the activity evades standard signature-based security prevent/detect solutions, or when it is not possible to use signature-based detection, for some reason.	COMPLETE
	When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.	PARTIAL

Requirement	Security Objectives	Nozomi Networks Support for OT/ICS Networks
Supply chain security	The organisation understands and manages security risks to networks and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers	COMPLETE
	Hardware and software resources used for administration purposes are managed and configured by the operator, or, where appropriate, by the service provider that the operator has authorised to carry out administration operations.	PARTIAL
Security in network and information systems	For each CIS and according to a number of indicators and assessment methods, the operator evaluates its compliance with its ISSP. Indicators may relate to the risk management organization's performance, the maintaining of resources in secure conditions, users' access rights, authenticating access to resources, and resource administration.	COMPLETE
	The operator develops and implements a procedure for security maintenance in accordance with its ISSP. To this purpose, the procedure defines the conditions enabling the minimum security level to be maintained for CIS resources.	COMPLETE
	Data stored or transmitted electronically is protected from actions such as unauthorized access, modification, or deletion that may cause disruption to essential services.	PARTIAL
Policies and procedures for cybersecurity risk management	The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.	PARTIAL
	The organisation monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and track the ongoing effectiveness of protective security measures.	COMPLETE
The use of cryptography and encryption	In its ISSP, the operator establishes and implements a policy and procedures related to cryptography, in view of ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information in the CIS.	PARTIAL

4.2. Highlight: Policies on Risk Analysis and Information Systems Security Policies

Operational technology, industrial control systems, and Internet of Things (IoT) devices are often insufficiently managed from a security perspective. Network maps may be missing, outdated, or have inaccurate asset inventories and lack detailed architecture diagrams and data flow diagrams. This missing data means that organisations do not have the required information to be able to drive effective governance or risk management. As a result, organisations are faced with the insurmountable task of generating and managing this information. The Nozomi Networks platform provides maximum visibility, vulnerability mapping, risk assessment and reporting tools.

Our platform creates a network diagram that includes precise and detailed asset information, including name, type, serial number, firmware version, and components. This data is obtained passively and automatically when the sensor is connected to a span or mirror port on the industrial network. A detailed data flow map is generated to help an organisation understand its conformance with internal policy, external regulations, and industry standards. We provide actionable risk assessment, insights including security and reliability alerts, missing patches and known vulnerabilities. With the detail provided, an organisation can begin to understand and identify assets that are critical to the operation of essential services, as well as security deficiencies.



The Nozomi Networks platform automatically maps and visualises an organisation's entire industrial network including assets, connections, and protocols. It continuously monitors network communications and behaviour to baseline 'normal' activity and alert on risks that threaten system reliability.

Cyber threats to critical assets become apparent and risk decisions become informed. Mitigations then deliver demonstrable risk reductions that can be clearly communicated to key stakeholders and auditors. Our global ecosystem of partners has been Nozomi Networks-certified to deploy on-premises, as part of a hybrid network, with SaaS resources, or manage it all for you. Additionally, Nozomi Networks can support all security needs, with professional service delivery and managed security services partners, along with integrated security technologies, and global, regional, and local channel and system integrator partners.

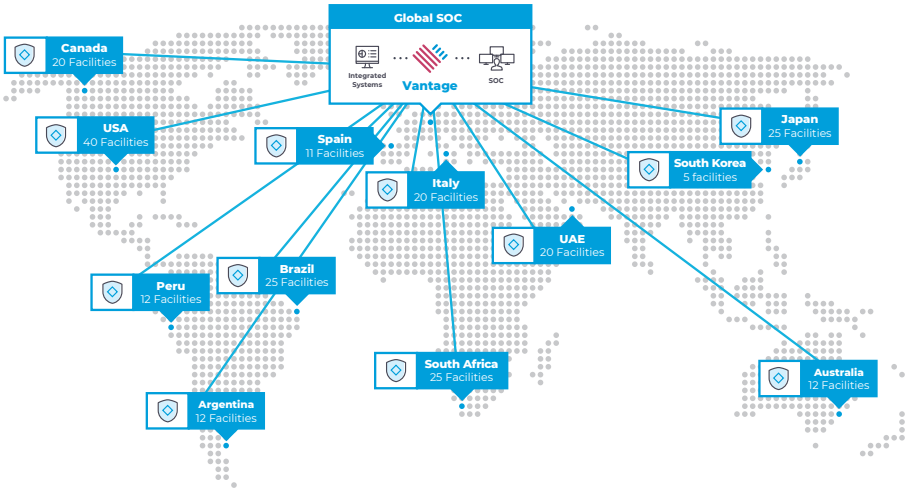
4.3. Highlight: Incident Handling with Nozomi Networks

The network mapping and visualization capabilities of the platform support best practices for network design – leveraging information on how traffic flows in existing and segmented networks. Our technology learns the normal operation of the network and process. Once the learning process has been completed, the system switches into protection mode which alerts users to changes in process and network behaviour. Network traffic flow can also be enforced with integration into next generation firewalls, creating a virtualized approach to network segmentation.

By combining AI and behaviour-based analytics with a rule-based threat detection mechanism, the Nozomi platform detects exploitation of vulnerabilities. This provides protection for known vulnerabilities in an environment where routine patching may not be possible. These same mechanisms also provide protection against known threats and malware as well as zero-day threats. This approach to network security means that should conventional protection mechanisms fail, attempted breaches are detected, minimizing any impact from attacks that would otherwise remain undetected.

The solution provides industry-leading alert capabilities with regards to incident management. Security alerts can be prioritized, resolved, and flagged, allowing incident responders to focus efforts on genuine security issues. In addition, our Threat Intelligence feed delivers up-to-date threat intelligence, making it easy to detect threats and identify vulnerabilities in OT and ICS environments. Threat Intelligence is produced and curated by the Nozomi Networks Labs team of expert security researchers. Nozomi Networks also supports the addition of custom signatures provided by industry sources working closely on threats specific to critical and industrial sectors.

Detailed event correlation and attack vector analysis enabled by Nozomi Networks appliances can be fed back into the incident response and security protection policies. This helps ensure that lessons are learned from security incidents and leads to a more robust cybersecurity posture going forward.



The Nozomi Networks Vantage SaaS product provides centralized access to data from all Guardian deployments in the field or on the plant floor across multiple sites.

With Vantage, our SaaS solution, implementation of policies and procedures can be verified, producing metrics that demonstrate risk reduction, such as reducing the number of critical vulnerabilities or unsupported operating systems. By providing detailed and accurate information in real-time, Vantage enables organizations to quickly detect and respond to cyber threats, risks, and anomalies with a scalable SaaS platform that consolidates OT and ICS security management into a single application.

4.4. Highlight: Business Continuity and Crisis Management with Nozomi Networks

Network mapping supports NIS2 requirements with respect to data storage and system dependency mapping. With this information, an organisation can better understand the impact of corruption or loss of availability of this data, enabling a focused and risk-based approach to the protection of critical services. Incident response processes can also be better informed and enabled to rapidly restore essential services following disruption.

Our platform provides detailed information across all aspects of an industrial network, logging granular details about each asset, its activity and traffic patterns, amounts of transferred data, protocols and function codes, source and destination ports, connection attempts, software and firmware versions and updates in real time. Detailed information on network traffic flow and dependencies and packet traces can also be downloaded from appliances and made available to security and forensics teams for in-depth packet level analysis.

The solution also ingests data in the form of network packet captures (PCAPs) and can be used to simulate an attack, as a training tool, and to help organisations exercise their incident response procedures – a requirement of NIS2.

The Nozomi Networks platform quickly detects cybersecurity and process reliability threats to an organisation's ICS, and blocks attacks when integrated with compatible firewalls.

5. Conclusion

The key to effective network monitoring and risk management lies in using information to inform an accurate risk view. If network activity is not monitored in real time, the status of assets is largely unknown, and whether or not they have vulnerabilities, these assets cannot be protected without the necessary visibility into their day-to-day functionality.

Based on comprehensive AI behaviour-based analytics and signature-based detection engines, the Nozomi Networks platform reliably detects security incidents, policy breaches and process anomalies that could affect the delivery of essential services. Covering the entire industrial control network environment, our technology learns and understands normal network and process behaviour. Any changes from known state result in alerts, allowing users to detect known “indicators of compromise” (IoCs) and novel threat attempts.

The Nozomi Networks platform is built with full control of its entire technology stack, including the firmware and operating system on the physical appliance, in addition to the software solution itself. The system is hardened and subject to regular in-depth security checking. Nozomi Networks manages system patching through product updates where required. This means that the total cost of ownership is minimized while still delivering a highly secure platform. The platform incorporates role-based access controls with Active Directory (AD) integration, providing control over security event management with access limited to those with a business need.

The Nozomi Networks solution provides detailed asset identification and network discovery that helps an organisation achieve deep visibility into the status of its industrial control networks. Armed with information, an organisation can identify risks and threats active in its environments. Insight also allows it to implement an effective and targeted mitigation program that maximizes the use of limited human resources, while making informed risk decisions that are both efficient and effective.

Let's get started

For more details on specific product support and deployment options, please reach out to your local Nozomi Networks sales teams or Nozomi Networks partner network.

Contact Us

nozominetworks.com/contact

Nozomi Networks accelerates digital transformation by protecting the world’s critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com