Version 1.0

Whitepaper

Achieving NIS2 Compliance with Omny

Understanding NIS2 and how to address is with the Omny Platform

Public

Public

omnysecurity.com

Table of Contents

Building a Secure Platform Whitepaper

An Introduction to Cyber Compliancy with Omny

In order to keep pace in an evolving technological world, the European Union has introduced a second set of regulations in the Network and Information Security Directive to address the accountability for cybersecurity practices in important and essential organizations. Building upon the success of its predecessor, NIS2 aims to establish a consistent and elevated standard of cybersecurity hygiene throughout the European Union. It identifies essential and important services, and mandates the implementation of suitable and proportional measures to effectively manage risks to the security of their network and information systems.

Omny will lead you through historic regulations to better set the stage of the reverberations of NIS2, along with the consequences of non-compliance. Details around the implications for Nordic countries, specifically Norway outside the EU, will be reviewed, followed by suggestions on how to comply and how Omny fits can help you do so.

An Overview of NIS2

In 2016, the EU introduced the first NIS Directive (“NIS1”) in response to escalating cyber threats, focusing on the safeguarding of essential services like water and power. NIS2 (published as Directive (EU) 2022/2555) succeeds NIS1 with broader and more rigorous requirements applicable to organizations defined as “Essential” and “Important”. As NIS2 becomes adapted law across Europe, organizations must ensure that they have the capabilities needed to meet the new requirements.

NIS2 aims to mature the cybersecurity posture of European organizations’ by:

- **Strengthening cybersecurity across critical sectors:** NIS2 ensures critical sectors like healthcare, energy, and transport are protected with enhanced cybersecurity measures to prevent disruptions from cyber threats.
- **Harmonizing cybersecurity standards across the EU**: NIS2 creates a unified framework for consistent cybersecurity practices across all EU member states, simplifying compliance for cross-border operations.
- **Improving incident reporting and cross-border collaboration**: NIS2 establishes clear reporting requirements and fosters collaboration to enable faster and more effective responses to cyber incidents.

Key Requirements in NIS2

NIS2 requires in-scope organizations to satisfy specific governance, risk management, and reporting capabilities and obligations:

Strengthening cybersecurity across critical sectors

Ensuring critical sectors like healthcare, energy, and transport are protected with enhanced cybersecurity.

Governance

Management is required to approve cybersecurity risk-management measures, including training for themselves and employees (Article 20).

Cybersecurity risk-management measures

Network and information systems must be protected from cyberthreats, physical security failures, human error, and natural disasters. Additionally, appropriate and proportionate technical, operational, and organizational measures must be in place to manage those risks (Article 21).

Reporting obligations

The timely notification of significant incidents (to CSIRT or equivalent authority), and formal reporting of significant incidents must occur. Notification to the recipients of services potentially affected by any incidents must also be notified, and potentially publicly disclosed (Article 23).

Harmonizing Cybersecurity standards across EU

NIS2 creates a unified framework for consistent cybersecurity practices across all EU member states, simplifying compliance for cross-border operations.

Improving incident reporting and cross-border collaboration

NIS2 establishes clear reporting requirements and fosters collaboration to enable faster and more effective responses to cyber incidents.

Similarities and differences between NIS1 and NIS2

NIS2 includes more context in order to be more prescriptive and specific than NIS1. The most important differences are the **broader scope** across more sectors, including the chemical and food industries. The **classifications** have been revised to distinguish between "operators of essential services" and "digital service providers," with essential entities subjected to more rigorous enforcement and oversight measures. NIS2 has **stricter mandates**, requiring more proactive cybersecurity obligations for essential and important entities. These entities must also follow **enhanced incident reporting** that requires the introduction of a multi-stage approach to **incident reporting**. It is important for organizations to follow new protocols to avoid penalties that accompany increased enforcement of these regulations. Management will also take on **increased accountability** for the upkeep of NIS2 and the reporting of breaches. Fortunately, however, NIS2 overlaps with other regulatory initiatives and is meant to avoid compliance-related inefficiencies.

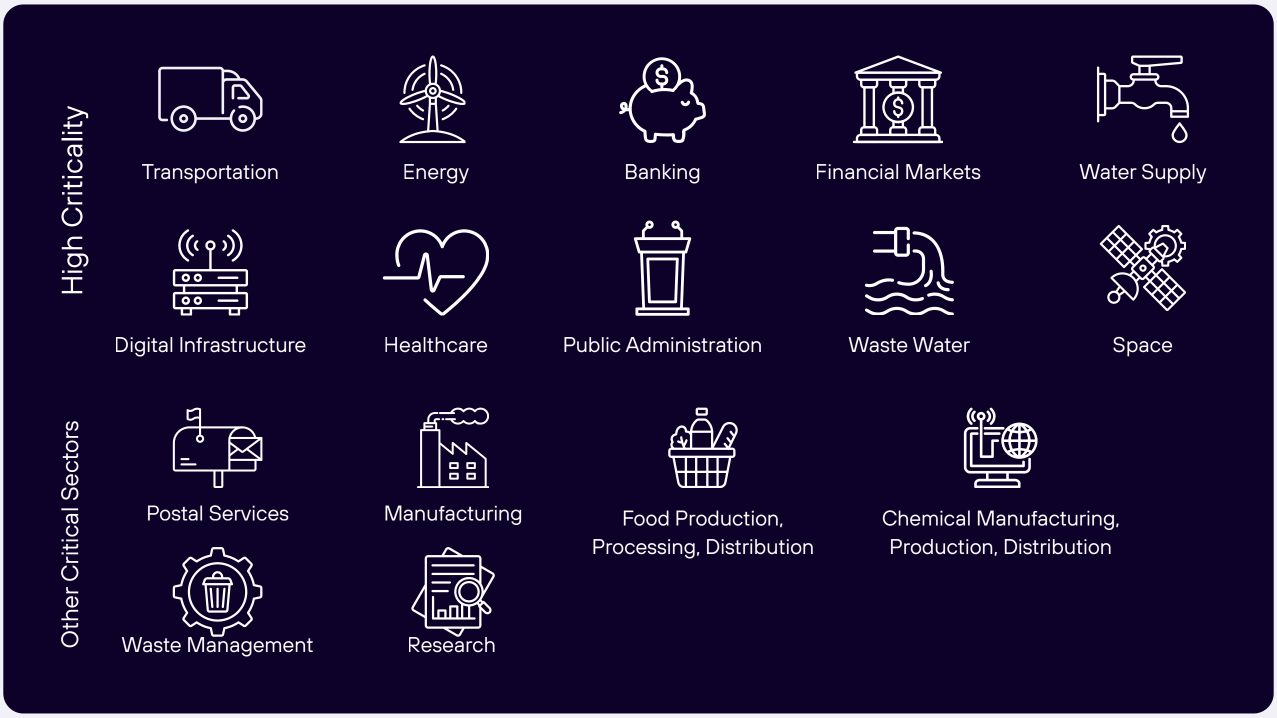
Does NIS2 apply to your organization?

NIS2 categorizes organizations into two categories, “essential” entities and “important” entities, based on their size and criticality. **Essential** entities are large enterprises operating in sectors of high criticality. **Important** entities are medium-sized enterprises operating in sectors of high criticality, or large enterprises operating in other critical sectors.

First, let’s understand the difference between the various sizes an organization can fall under using the chart below.

Size Category	Number of employees	Turnover and/or Balance
Large enterprise	> 250 persons	Revenue > EUR 50M or Balance > EUR 43M
Medium enterprise	50-250 persons	Revenue between EUR 10-50M or Balance between 10-43M
Small enterprise	10-50 persons	Revenue and/or Balance EUR 2-10M
Micro enterprise	< 10 persons	Revenue and/or Balance < EUR 2M

Secondly, use the below chart to determine which sector you fall under. If in doubt whether your enterprise is included in a sector, reference the EU's database for statistical classification of economic activities (called "NACE").



High Criticality

Transportation

Energy

Banking

Financial Markets

Water Supply

Digital Infrastructure

Healthcare

Public Administration

Waste Water

Space

Other Critical Sectors

Postal Services

Manufacturing

Food Production, Processing, Distribution

Chemical Manufacturing, Production, Distribution

Waste Management

Research

Essential entities and Important entities

NIS2 categorizes organizations into *Essential* and *Important* entities based on their size and criticality. Essential entities are Large enterprises operating in Sectors of High Criticality. Important entities are Medium-sized enterprises operating in Sectors of High Criticality, or Large enterprises operating in Other Critical Sectors.

Size Category	Sectors of High Criticality	Other Critical Sectors	Other Sectors Selected by Member States
Large enterprise	Essentail	Important	Essential or Important
Medium enterprise	Important	Important	Essential or Important
Small enterprise	N/A	N/A	Essential or Important
Micro enterprise	N/A	N/A	Essential or Important

There are certain exceptions to these categorizations, as determined by national authorities based on specific localized criteria, such as the significance of their services for public safety, security, or health. Refer to Article 3 in the Directive.

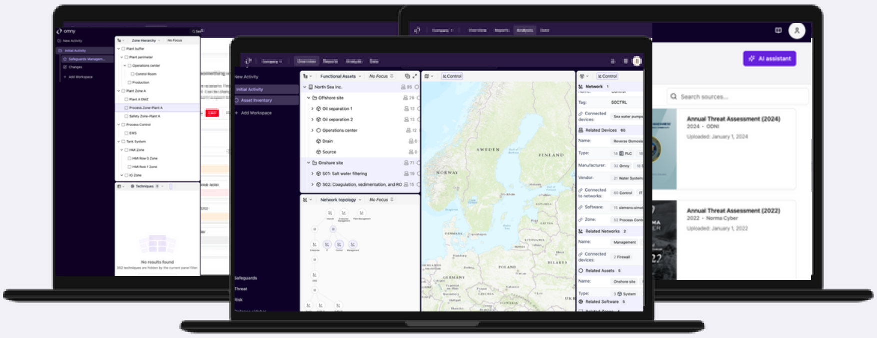
Organizational penalties and personal liability

While the key requirements for Essential entities and Important entities are the same, they face different supervision measures and penalty levels.
Management may also be held personally liable for infringements.

- For **Essential entities**: Administrative fines can be imposed up to €10,000,000 or at least 2% of the total annual worldwide turnover in the company's previous fiscal year to which the essential entity belongs (whichever amount is higher).
- For **Important entities**: Administrative fines can be imposed up to €7,000,000 or at least 1.4% of the total annual worldwide turnover in the company's previous fiscal year to which the important entity belongs (whichever amount is higher).

How Omny helps you achieve NIS2 compliance

Achieving compliance will require planning and prioritization to make the best use of your time and resources. We recommend starting with the following steps:

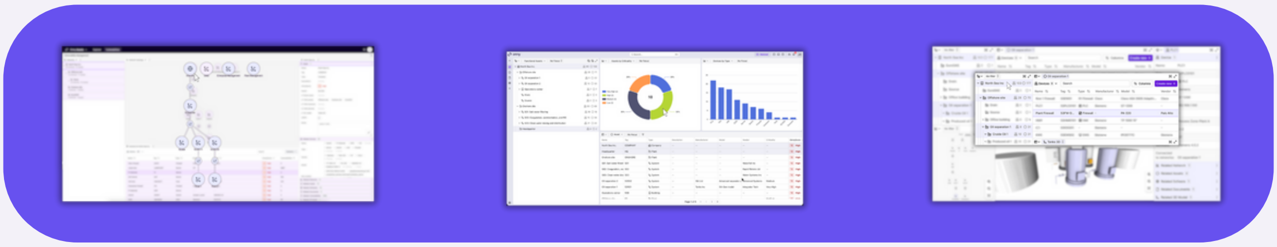

AI assistant
Annual Threat Assessment (2024)
Annual Threat Assessment (2022)

1. **Perform a readiness and maturity assessment** - Assess your NIS2 readiness using our 6-minute NIS2 Readiness Quiz. Then perform a maturity assessment against an appropriate cybersecurity framework or standard.
2. **Get everyone on board** - NIS2 compliance requires the active involvement from people at all levels across the organization, particularly leaders.
3. **Choose a monitoring tool** - The broad scope of NIS2 requirements will have a large footprint on your organization. You will therefore need a tool that enables accurate monitoring and reporting of your compliance program's status.

Omny's Capabilities

The Omny platform streamlines the processes and operational activities required by NIS2 Articles 20, 21 and 23. The platform will help you:

- **Streamline compliance work and reporting** with cybersecurity regulations such as NIS2, and relevant frameworks (e.g. IEC 62443, NIST CSF) through simplified and automated assessments, documentation, reporting and improvement flows.
- **Maintain continuous visibility** into your cybersecurity posture with dynamic dashboards and asset-level scorecards that highlight status, compliance and control gaps, and recommendations to increase maturity and improve security.
- **Identify and prioritize improvements** through clear, guided roadmaps that reduce audit effort and operational disruption.
- **Proactively manage risk** and effectively present maturity and compliance status to regulators, customers, and other stakeholders.



The Omny platform includes several main use cases, assisted by AI powered workflows that guide you through:

- **Compliance and Maturity:** Continuously track and demonstrate maturity and compliance against legal obligations and industry leading standards and frameworks. Identify gaps and track improvement.
- **Risk Management**: Identify top cyber-physical risks faster based on updated operational security status and threat level, enabling better risk-based decision making.
- **Asset Inventory**: Unify and gain actionable insights from siloed cybersecurity and operations data scattered across multiple point solutions, aiding business continuity and incident management.
- **Vulnerability Handling**: Reduce time spent on understanding vulnerability exposure and exploitability of CVEs, enable ability to keep an appropriate level of security.
- SOC Enhancement: Support NIS2 reporting obligations (in Article 23) through faster triaging of alarms in cross-domain SOC, with documented and auditable decisions, aiding business continuity and incident management.

The Omny Platform also offers a suite of built-in assessment profiles:

Maturity Assessment

Assessment of the maturity of IACS service providers against the ISA/IEC 62443-2-4 standard and also NIST CSF.

Gap Assessment

Assessment of gaps against the system security requirements in the ISA/IEC 62443-3-3 standard.

Business Impact Assessment

Assessment of the business impact (financial, safety, environmental) of incidents (i.e., downtime as a result of Loss of Control) for key assets at a site.

Threat Assessment

Evaluation of potential cyber threats to the company's critical assets and operations, aligning with the MITRE ATT&CK framework.

Risk Assessment

Visualized scenario-based assessment of security risks for industrial assets, enabling a risk-driven approach to industrial security management.

Professional Services

From complexity to confidence, we will assist you in improving your security posture and maintaining up-to-date documentation of your compliance status. There are a lot of uncertainties around NIS2. Knowing how this Directive will affect your business can be difficult to understand. Why not start with a discussion around your NIS2 compliance needs?

The Omny Professional Services team is a group of trusted experts within governance, risk and compliance, industrial cybersecurity, and threat intelligence guiding you and your team on your security maturity journey. We will help you scale your security work through deep domain expertise and powerful industrial technology.

About Omny

Omny is on a mission to make sense of increasingly complex threats to society's most critical infrastructure. Our software leverages the latest advancements in data science and technology to mitigate these threats. Born from the industry and built on domain expertise, Omny is positioned to help companies face their cyber challenges. Omny has an international vision with its headquarters in Oslo, Norway and an additional office in Stavanger, Norway.

To learn more about our products and services, find us at omnysecurity.com or reach out to us at info@omnysecurity.com.

omny