sumo logic

# NIS2 compliance guide

## How to get and stay compliant

**This EU directive requires companies of all member states and their supply chains to be compliant by 17 October 2024.**

# What is NIS2?

NIS2 namely Network and Information Security Directive is the expanding version of the previous NIS directive, designed to enhance cybersecurity preparedness among European Union member states.

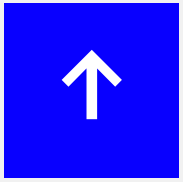
The proliferation of network and information systems, fueled by swift digital transformation and societal interconnectivity, exposes a growing array of impactful cyber threats.

The primary goal of this directive is safeguarding the internal market, as incidents can impede economic activities, result in financial losses, undermine user confidence, and harm the overall economy and society of the Union.

**Due to global interconnection, these regulations extend their reach, impacting supply chain providers from non-EU companies that primarily serve/operate or work with countries within the EU.**

## What are the key differences between NIS and NIS2?


**NIS2 doubled the number of sectors affected**



**Expanded and stricter requirements**


**Heavier fines for non-compliance**

# Who will be affected?

NIS2 divides the affected entities into two main categories: essential entities and other critical sectors.

**Essential entities:**
Size threshold: varies by sector, but generally a minimum of 250 employees, annual turnover of €50 million, or balance sheet of €43 million.

**Other critical sectors:**
Size threshold: varies by sector, but generally 50 employees, annual turnover of €10 million or balance sheet of €10 million.

**Note:**
An entity may still be considered essential or important even if it does not meet the size criteria, in specific cases such as when it is the sole provider of a critical service for societal or economic activity in a Member State.

## ESSENTIAL ENTITIES

- **Energy**
- **Transport**
- **Finance**
- **Public administration**
- **Health**
- **Aerospace**
- **Water supply** (drinking and wastewater)
- **Digital infrastructure** (cloud computing service providers and ICT management)

## OTHER CRITICAL SECTORS

- **Postal services**
- **Waste management**
- **Chemicals**
- **Research organisations**
- **Foods**
- **Manufacturing** (machinery, medical devices, vehicles/ transportation, and other equipment)
- **Digital providers** (social networks, search engines, online marketplaces)
- **Plus all sectors under “essential entities” and within the size threshold for “important entities”**

# 9 Important requirements you should know

*Please note that no single solution will make you totally NIS2 compliant, but Sumo Logic's solutions can help you meet some of the complex requirements. As you go through the requirements, you will see how we can support you on the way to becoming NIS2 compliant.

## 1

**Ensure risk analysis and information security policies are documented, communicated, and regularly assessed.**

## HOW SUMO LOGIC CAN HELP

**We can help you in documenting, communicating and assessing these policies:**

**Log Analytics Platform:** Leverage log data for faster threat detection, helping IT, DevOps, and SecOps teams focus on critical security events. Machine learning and automation streamline responses to high-impact threats.

**Cloud SIEM:** Built-in automation enriches alerts and uses playbooks to prioritize and accelerate incident investigation and remediation workflows.

**Logs for Security:** AI-driven alerts and risk scoring prioritize risks and 500+ pre-built security policy checks for easy policy enforcement across your cloud environment.

## 2

**Establish incident handling procedures and ensure reporting, document detection, triage, response actions, and preventive measures are in place.**

## HOW SUMO LOGIC CAN HELP

**Threat detection, investigation, and response:**

Cloud SIEM gives SOC analysts prioritized and contextualized actionable threats with automated security workflows.

View, explore, and report on how entities are connected with the Entity Relationship Graph. Get a panoramic visualization to see the full scope and breadth of a cyber breach.

Enhance detection with 900+ out-of-the-box integrations and content rules and instantly comprehend the scope of detection with MITRE ATT&CK coverage explorer.

Automatically enriched Insights power playbooks for deeper context for investigations and integrated automation for containment actions.

Additional response automation with Cloud SOAR fully automates the triage, investigation, and remediation of threats for any security professional.

## 3

**Implement and maintain backup management and disaster recovery processes to ensure business continuity during and after security incidents.**

### HOW SUMO LOGIC CAN HELP

**Log data, alerts, and automated incident reports:**

Automated incident reports reduce noise so teams can focus on relevant events.

Reduce Mean Time to Resolution (MTTR) with the patented LogReduce technology that reduces hundreds of thousands of pages of results into a handful of meaningful patterns.

Security data lake keeps all aggregated log data, both structured and unstructured, secured and readily available without the need for cold storage or rehydration. This speeds investigations and supports business continuity processes by ensuring data availability.

## 4

**Supply chain security is a must-have: Identify and mitigate supply chain risks, assess security measures for all suppliers, and implement a continuous supplier risk assessment plan.**

### HOW SUMO LOGIC CAN HELP

We can only advise organizations to confirm where or how a business operates to ensure a compliant supply chain. You may have to evaluate or even change some suppliers.

This will also increase the directive's scope and have a greater impact on suppliers outside of the EU who tend to have a customer base in any of the member states.

5

**Ensure security around the procurement, development, and operation of information systems by creating policies for handling and reporting vulnerabilities.**

## HOW SUMO LOGIC CAN HELP

Logs for Security accelerates security visibility for your development, operations, security, and reliability management teams, managing your risk and attack surface.

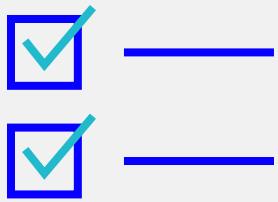
Cloud SIEM automated incident reports help with noise reduction to focus on relevant events.

MITRE ATT&CK identifies areas of strength, uncovers gaps in your defenses, and prioritizes enhancements based on the evolving threat landscape. Provides guidance on best practices and known attacks based on similar organizations (threat benchmarking).

Our Signal clustering algorithm automatically groups related Signals, accelerating alert triage. Once the aggregated risk surpasses a threshold, it automatically generates an Insight to help you focus.

Insight Confidence scores, predicted by Sumo Logic's Global Intelligence machine learning model, help you triage and prioritize Insights.

Sumo Logic's threat intelligence provides a comprehensive threat intelligence aggregator, enabling users to analyze, leverage, and act on threat data for enhanced security.



## 6

**Establish policies and procedures to assess the effectiveness of risk-management measures.**

### HOW SUMO LOGIC CAN HELP

We cannot establish these policies and procedures as such.

However, having DevSecOps in one platform makes reporting procedures and risk assessment across cross-functional teams easier. With unlimited users and cutting-edge AI-powered log analytics, your teams can ingest everything and build a single source of truth, facilitating your assessment across various teams.

Logs for Security can help here: risk scoring and alert prioritization, anomaly detection, and AI-driven alerting to assess risks before they turn into incidents improves effectiveness and ensures you have the audit logs needed to assess these measures.

## 7

**Make sure you conduct cyber hygiene practices such as cybersecurity awareness training within your business.**

### HOW SUMO LOGIC CAN HELP

Sumo Logic offers certification courses in all our products to ensure security practitioners are well-versed in the features and capabilities of our product suite. These courses can also be used to inform security policies and best practices within their organization.

*We can only advise to have this in place.*

## 8

**Establish policies and procedures for the use of cryptography and, when relevant, encryption.**

### HOW SUMO LOGIC CAN HELP

Sumo Logic encrypts all data at rest (AES 256) and in transit (TLS) to ensure data remains confidential.

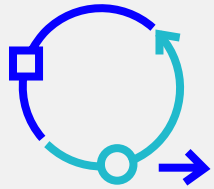
## 9

**Use multi-factor authentication or continuous authentication solutions throughout the business.**

### HOW SUMO LOGIC CAN HELP

*While Sumo Logic doesn't offer MFA solutions, we can ingest MFA logs, including those from top providers like Okta. These logs can ensure and prove that policies are enforced across your organization.*

Logs for Security and Cloud SIEM can ingest MFA (Okta, etc.) logs. These logs can help you prove that the policies are enforced across the organization.



## Enforcement

The NIS2 Directive emphasizes supervision and enforcement by competent authorities across EU Member States. It sets minimum supervisory measures for essential entities, introducing differentiated regimes for a balanced approach.

The directive addresses historical reluctance to penalize entities, establishing a consistent EU-wide framework for sanctions, including fines based on turnover.

**Essential entities may face fines up to €10,000,000 or 2% of their total annual turnover, and important entities up to €7,000,000 or 1.4% of turnover, promoting accountability for organizational cybersecurity measures.***

To improve compliance, NIS2 outlines minimum supervisory tools, such as audits, inspections, and information requests, while differentiating between essential and important entities.

On enforcement, the Directive addresses the reluctance of member states to apply penalties for security failures.

**It introduces a unified sanction framework, including fines, security audits, and orders to comply with NIS requirements.**

For essential entities, fines can reach up to €10 million or 2% of global turnover, and for important entities, up to €7 million or 1.4%.

## Responsibilities and liabilities for executive staff

Senior managers may also be held liable for cybersecurity breaches if they don't fulfill their obligations under this directive.

**Article 32(6) of the NIS2 Directive** explicitly provides for liability in the context of essential entities: *"Member States shall ensure that any natural person who is responsible for an essential entity or acts as a representative of the essential entity based on their authority to represent, make decisions on behalf of, or exercise control over the entity, is empowered to ensure that the entity complies with this Directive.* ***Member States shall ensure that such natural persons can be held liable*** *for breaches of their duties to ensure compliance with this Directive."*

**Managers and leadership teams are therefore responsible for approving cybersecurity measures, monitoring how they're put into practice, and can be held accountable if these measures don't meet the requirements of the NIS2 directive.**

Furthermore, leadership teams of essential and important organizations have to undergo cybersecurity training and are encouraged to provide regular training for their employees as well. This way, both leaders and employees can build the skills to identify risks, evaluate cybersecurity practices, and understand how these practices impact the organization's services.

## Interaction with other EU Regulations

The NIS2 Directive is closely tied to two other initiatives:

The Critical Entities Resilience (CER) Directive NIS2 and the CER Directive align their scopes to comprehensively address the physical and cyber resilience of critical entities. Entities identified as critical under the CER Directive will also be subject to NIS2 cybersecurity obligations. National competent authorities under both directives must regularly cooperate and exchange information on cyber and non-cyber risks.

The Regulation for Digital Operational Resilience for the Financial Sector (DORA).

The new NIS2 Directive covers credit institutions, trading venues, and central counterparties in the financial sector, while DORA specifically addresses its cybersecurity risk management and reporting obligations. To ensure effective information exchange between the financial sector and other NIS2 sectors, DORA allows European Supervisory Authorities and national authorities to participate in NIS Cooperation Group discussions. DORA authorities can also consult and share information with NIS2 Single Point of Contacts (SPOCs) and CSIRTs. Details of major ICT-related incidents will be shared between competent authorities under DORA and those established under NIS2. Member States are encouraged to include the financial sector in their cybersecurity strategies, and national CSIRTs may encompass the financial sector in their activities.

The NIS2 Cooperation Group and the Critical Entities Resilience Group under the CER Directive will meet at least once per year to facilitate collaboration.

**Learn how OpenPayd streamlined its compliance efforts with Sumo Logic.**

**If you have any questions, please contact us directly or enquire about a product demo tailored to your requirements.**

*source:https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

## About Sumo Logic

Sumo Logic helps make the digital world faster, reliable and more secure. Through its AI-powered SaaS Log Analytics Platform, organizations can unify and analyze enterprise data, translating it into actionable insights. This single source of truth enables Dev, Sec and Ops teams to simplify complexity, collaborate efficiently and accelerate data-driven decisions that drive business value. Customers around the world rely on Sumo Logic to ingest and analyze logs, events, metrics, traces and other data sources at scale to ensure application reliability, secure and protect against modern security threats, and gain insights into their cloud infrastructures. **For more information, visit www.sumologic.com.**

sumo logic