



WHITEPAPER

NIS2 Directive

Getting ready for compliance with Sekoia

Prepared by Sekoia

White paper · Compliance · Public

CONTENTS

Table of contents

The three pillars of NIS2.....	3
Scope: who is concerned?.....	4
Sectors of high criticality and other critical sectors.....	4
Sectors covered by NIS2.....	4
Important and essential entities.....	4
Cybersecurity requirements.....	6
The ten risk-management measures.....	6
Timeline.....	7
Notification of significant incidents.....	8
Responsibility of executives.....	8
Sanctions.....	9
How Sekoia supports your NIS2 compliance.....	10
Appendix – How the Sekoia AI SOC platform answers NIS2 requirements.....	12
Other NIS2 measures.....	15
About Sekoia.....	16

The European Union adopted a landmark directive at the end of 2022 to protect all major sectors of the European economy from cyber threats. Directive (EU) 2022/2555 - better known as NIS2 (Network and Information Security 2) — establishes a high common level of cybersecurity for networks and information systems across the EU. Member States were required to transpose it into national law by 17 October 2024, and its measures have applied since 18 October 2024, when the previous NIS1 Directive (Directive (EU) 2016/1148) was repealed. Several Member States transposed the directive after the deadline, and the European Commission has opened infringement proceedings against those that were late.

Because the directive now applies and national enforcement is under way, organizations in scope should not delay the work of planning, implementing and testing the necessary tools, strategies and procedures. This guide presents the main changes brought about by NIS2 and explains how Sekoia can help you bring your organization into compliance.

AT A GLANCE

The three pillars of NIS2

Responsibilities of Member States	Risk management	Cooperation and information sharing
▶ National authorities ▶ National strategies ▶ Coordinated vulnerability disclosure (CVD) ▶ Crisis management	▶ Responsibility of executives ▶ Risk management measures for Essential and Important Entities ▶ Incident notification within a short timeframe	▶ Cooperation Group ▶ CSIRT Network ▶ CyCLONe Network ▶ EU database of known vulnerabilities ▶ Peer reviews

Private companies and public organizations are mainly concerned by this second pillar — risk management.

SCOPE

Scope: who is concerned?

Sectors of high criticality and other critical sectors

To ensure the continuity of services and the proper functioning of the European economy, the NIS2 Directive expands the list of critical sectors which must be protected from threats to networks and information systems. Thus, new sectors such as wastewater, agri-food but also public administration are now covered.

A NEW PARADIGM

Over 300,000 organizations are expected to be covered by NIS2 across Europe, compared with a few thousand under NIS1.

Sectors covered by NIS2

Detailed in Annex 1 and Annex 2 of the directive, the covered sectors now span eighteen domains:

▶ Energy	▶ Transport	▶ Banking
▶ Financial market infrastructures	▶ Health	▶ Drinking water
▶ Waste water	▶ Digital infrastructure	▶ ICT service management
▶ Public administration	▶ Space	▶ Postal and courier services
▶ Waste management	▶ Chemicals - manufacture, production & distribution	▶ Food - production, processing & distribution
▶ Manufacturing	▶ Digital providers	▶ Research

The directive distinguishes sectors of high criticality (Annex I) from other critical sectors (Annex II); several of these were newly brought into scope by NIS2.

Important and essential entities

Under NIS1, entities were classified as Operators of Essential Services (OES) and Digital Service Providers (DSP). NIS2 now classifies entities as "essential" or

“important” within the sectors above, reflecting the criticality of their services and taking into account their sector of activity, size and turnover.

Classification broadly follows a size-cap rule. In the sectors of high criticality (Annex I), large enterprises (as a rule, 250 or more employees, or annual turnover above €50M and a balance-sheet total above €43M) are essential, while medium-sized enterprises are important. Entities in the other critical sectors (Annex II) are generally important. Some entities are essential regardless of size, however — for example DNS service providers, TLD name registries, qualified trust service providers, providers of public electronic communications networks, and, in many Member States, central public administration.

The main differences between essential and important entities lie in the measures to be implemented and in the way compliance is supervised. Essential entities are subject to proactive (ex ante) supervision — they are actively monitored to verify compliance. Important entities are supervised ex post, where signals of an incident have appeared. If it emerges after an incident that the necessary measures were not taken, the organization may receive a fine and/or other sanction imposed by the national authority.

THE SUPPLY CHAIN IS ALSO COVERED

Managed service providers and managed security service providers (MSPs and MSSPs) are explicitly in scope and must comply with security requirements.

NIS2 also aims to secure the wider supply chain: essential and important entities are expected to address security in their relationships with their own suppliers and service providers.

FINANCIAL SECTOR — DORA TAKES PRECEDENCE

For financial entities, Regulation (EU) 2022/2554 (DORA) has applied since 17 January 2025 and operates as sector-specific law (lex specialis) that prevails over NIS2 for ICT risk management and incident reporting (NIS2, Article 4).

Banking and financial market infrastructures should therefore look primarily to DORA for their ICT obligations.

REQUIREMENTS

Cybersecurity requirements

Organizations covered by NIS2 must implement an active cyber protection strategy that includes prevention, detection, monitoring, analysis and mitigation.

The ten risk-management measures

Ten major “cybersecurity risk-management measures” are listed in Article 21 of the directive:

01	Policies on risk analysis and information system security
02	Incident handling
03	Business continuity, including backup management, disaster recovery and crisis management
04	Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
05	Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
06	Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
07	Basic cyber hygiene practices and cybersecurity training
08	Policies and procedures for the use of cryptography and encryption
09	Human resources security, access control policies and asset management
10	Use of multi-factor authentication (MFA) or continuous authentication solutions, secured voice, video and text communications

Timeline

17 Oct 2024	Transposition deadline. NIS2 measures apply from 18 October 2024, when the NIS1 Directive (2016/1148) was repealed. Several Member States transposed after this date.
17 Oct 2024	Commission Implementing Regulation (EU) 2024/2690 adopted — it sets the technical and methodological requirements for DNS, cloud, data-centre, content-delivery-network, managed service and managed security service providers, online marketplaces, search engines, social-media platforms and trust service providers, and defines what counts as a “significant incident” for them.
17 Jan 2025	DORA (Regulation (EU) 2022/2554) becomes applicable and takes precedence over NIS2 for the financial sector.
Ongoing	National transposition, registration of entities and sector-specific rules continue to be finalised and enforced across the EU.

These EU-wide measures are translated into national referentials and specified by regulation. In France, for example, they take the form of “compliance objectives” within the new ReCyF framework. See also the Appendix for how Sekoia responds to these technical and governance requirements.

THESE MEASURES SHOULD

- ▶ *Be proportionate to the risk, cost, impact and severity of incidents*
- ▶ *Take into account the state of the art and, where applicable, relevant European and international standards*

THE EU CAN

- ▶ *Conduct risk assessments related to critical services, ICT systems or supply chains*
- ▶ *Impose certification obligations*
- ▶ *Adopt implementing acts setting out technical requirements*

INCIDENT REPORTING

Notification of significant incidents

NIS2 imposes phased reporting obligations on essential and important entities, for incidents that have a "significant impact" on the provision of services. These notifications must be addressed to the competent authority or the CSIRT.

Within 24h	Early warning <i>Is there a suspicion of a malicious action likely to have cross-border repercussions?</i>
Within 72h	Incident notification <i>Assessment of the incident, its severity and impact; sharing of indicators of compromise (IoC).</i>
Upon request	Intermediate report <i>Upon the request of a CSIRT.</i>
1 month	Final report <i>Within one month of the 72-hour incident notification. If the incident is still ongoing at that point, a progress report is submitted instead, followed by a final report within one month of the incident being handled.</i>

Where applicable, entities inform the recipients of their services of significant incidents. Where the public interest warrants it, the CSIRT or competent authority may notify the public of the significant incident or require the entity to do so.

Responsibility of executives

Senior managers are ultimately responsible for managing cybersecurity risks in critical and important entities. Management bodies will have to approve the risk-management measures and supervise their implementation in the entity. CEOs (natural persons) may be held personally liable for a violation of the NIS2 directive by the company, and may be temporarily suspended from carrying out their duties. They are also required to undertake cybersecurity training and provide it to their employees.

Sanctions

The directive raises the ceiling for sanctions that can be imposed by the national authority:

- ▶ Up to €10,000,000 or 2% of total worldwide annual turnover (whichever is higher) **for essential entities.**
- ▶ Up to €7,000,000 or 1.4% of total worldwide annual turnover (whichever is higher) **for important entities.**

In addition to financial sanctions, States will have the possibility to issue warnings and take other restrictive measures, such as withdrawal of certification, in the event of violation of the NIS2 Directive.

SEKOIA & NIS2

How Sekoia supports your NIS2 compliance

Are you classified as an essential or important entity? Sekoia allows you to improve your protection by making it easier to detect and respond to cyberthreats. More specifically, our Sekoia Intelligence and Sekoia AI SOC platform solutions help meet many NIS2 requirements (see details in the appendix):

- ▶ **Risk assessment:** Knowledge of attackers thanks to cyber threat intelligence (Sekoia Intelligence) allows, at a strategic and operational level, a better understanding of the risks your organization faces.
- ▶ **Incident handling:** Real-time event monitoring, security incident detection and response automation with Sekoia AI SOC platform. Detection rules are continually developed and updated to support implementation of the directive in a company or public organization.
- ▶ **AI-assisted investigation and triage:** Sekoia Elevate, our agentic AI layer, investigates and triages alerts automatically. What used to take hours now takes minutes, leaving analysts with 90% less manual triage effort. This directly supports the incident-handling and short notification timeframes required by NIS2.
- ▶ **Notification to authorities:** With Sekoia Elevate automating investigation, the assessment that used to take hours now takes minutes (roughly 5x faster). Teams reach a clear view of severity and impact well inside the 24h early-warning window.
- ▶ **Information sharing:** The standardization of information on the Sekoia AI SOC platform makes it easier to report incidents and share information on cyber threats promoted by the directive.
- ▶ **Business continuity:** Sekoia Intelligence helps you develop relevant crisis-management exercises, while Sekoia AI SOC platform provides a tool to carry them out - for example, the platform is used by NATO as part of the Crossed Swords exercises.

A trusted partner for the resilience of your organization

Sekoia is already implementing best practices in security assurance (MFA, intrusion testing, etc.) and secure platform engineering.

- ▶ **Cloud security:** The platform can benefit from qualified SecNumCloud hosting, which guarantees strict standards and good practice in data security.
- ▶ **Certifications:** Sekoia is certified according to ISO 27001, SOC 2 report, ENS (Spain) PCI-DSS (banking) standards in certain cloud regions.
- ▶ **Internal CERT:** Sekoia also operates its own CSIRT, itself a recognized member of InterCERT.

To know more, visit <https://trust.sekoia.com>

“The NIS2 Directive should not be approached as a compliance issue, but as an opportunity to improve the level of cybersecurity.”

APPENDIX

Appendix – How the Sekoia AI SOC platform answers NIS2 requirements

Standard information security frameworks such as ISO/IEC 27001, PCI-DSS or NIST can be used to prepare for NIS2, identify technological and organizational gaps, and implement compliance efforts. The table below maps NIS2 requirements to the corresponding ISO 27001 security domains. The third column indicates how Sekoia solutions contribute to the compliance of your own organization.

Note: the Annex A references below follow the ISO/IEC 27001:2013 structure.

Risk-management measures (Art. 21 NIS2)	ISO27001 Annex	How Sekoia helps
A) Policies on risk analysis and information system security	A.5 – Information security policies	Risk assessment: Knowledge of threats thanks to threat intelligence allows, at a strategic and operational level, a better understanding of the risks your organization faces. The FLINT reports (Flash Intelligence reports) integrated into the Sekoia offering aim precisely to provide a strategic vision of the threat to decision-makers. Sekoia Intelligence
B) Incident handling	A.16 – Information security incident management	Real-time supervision: The Sekoia platform allows events to be monitored in real time and security incidents to be detected as quickly as possible (KPI: MTTD ~3 sec). Sekoia Defend Detection: Sekoia provides numerous detection rules in a simple, interoperable and open format (SIGMA), immediately actionable. New rules will be developed to facilitate the implementation of the directive. Sekoia Intelligence Sekoia Defend Automated investigation (agentic AI): Sekoia Elevate runs first-level investigation and triage on alerts, cutting investigation time from hours to minutes (roughly 5x faster) and removing up to 90% of manual triage effort. Analysts focus on confirmed, contextualized incidents. Sekoia Elevate Response: With its SOAR module, the Sekoia platform allows you to respond more quickly to incidents and automate the response thanks to

Risk-management measures (Art. 21 NIS2)	ISO27001 Annex	How Sekoia helps
		playbooks and 300+ integrations. Sekoia Defend
C) Business continuity, including backup, disaster recovery and crisis management	A.17 – Business continuity aspects related to information security	Crisis exercises: Threat intelligence helps you develop relevant crisis-management exercises based on real cyber threats, while the SOC platform gives you a tool to carry them out. Sekoia Intelligence Sekoia Defend Crisis management: The SOAR module makes it possible to define playbooks in response to an identified crisis scenario and to automate the response. Sekoia Defend Resilience: The Sekoia platform is designed to be adaptable and redundant, and the logs it processes are hosted on the cloud. This contributes to the resilience of the organization in the event of a major crisis such as ransomware. Sekoia Defend
D) Supply chain security, including relationships with direct suppliers or service providers	A.15 – Relations with suppliers	Monitoring of third-party tools: The SOC platform has over 300 connectors to cover a large security perimeter, and can deploy a new architecture in a few hours. Sekoia Defend
E) Security in acquisition, development and maintenance, including vulnerability handling and disclosure	A.12 – Operational safety A.14 – Acquisition, development and maintenance of systems	Logging: The Sekoia platform, which can be integrated with a third-party log sink, allows logs to be retained for a specific period as required by law, as well as certifications such as ISO27001 or PCI-DSS. The log correlation and analysis system then helps to improve detection. Sekoia Defend Sekoia Exalog Platform security: Sekoia's CI/CD approach (continuous distribution and deployment) and its security posture allow you to have a hardened and constantly updated security system. Sekoia Intelligence Sekoia Defend Exposure and vulnerability context: Sekoia Reveal surfaces asset exposure and vulnerability context, helping teams prioritize remediation and feed vulnerability handling. Sekoia Reveal

Risk-management measures (Art. 21 NIS2)	ISO27001 Annex	How Sekoia helps
F) Policies and procedures to assess the effectiveness of risk-management measures	A.5 – Information security policies	Reporting: Mapping your detection effort according to the MITRE ATT&CK framework allows you to identify the actual level of coverage in your perimeter. Sekoia Defend
G) Basic cyber hygiene practices and cybersecurity training	—	Cyber hygiene: Setting up a SOC with a state-of-the-art security solution is a good practice for ensuring the cyber hygiene of an organization. Sekoia Defend
H) Policies and procedures regarding the use of cryptography and encryption	A.10 – Cryptography	Encryption: The Sekoia platform uses encryption of data in transit and at rest. Sekoia Intelligence Sekoia Defend
I) Human resources security, access control policies and asset management	A.5 – Information security policies A.7 – Staff safety A.8 – Asset management A.9 – Access controls A.11 – Physical & environmental security	Asset and identity context: Sekoia Reveal builds internal context across assets, identities and exposure. You can inventory what runs on the information system and shape asset-management and access-control policies accordingly. Sekoia Reveal
J) Use of MFA or continuous authentication, and secured communication systems	A.13 – Communications security	MFA: The Sekoia platform implements multi-factor authentication and SSO. Sekoia Intelligence Sekoia Defend

Other NIS2 measures

Notification of significant incidents (Article 23): Essential and important entities must notify the CSIRT of “significant” incidents with an early warning within 24 hours, then an incident notification within 72 hours. They must also inform the recipients of their services.	Notification within 24h: Sekoia Elevate investigates and triages incoming alerts automatically, so the organization reaches a severity assessment in minutes rather than hours (roughly 5x faster). The natively integrated CTI provides the 360° context needed to decide whether to file an early warning. Sekoia Intelligence · Sekoia Elevate. Sekoia Intelligence Sekoia Elevate Incident notification: Taking advantage of the platform’s automation capabilities, Sekoia offers creating playbooks to facilitate notification to authorities. Sekoia Defend Final report: Drafting is facilitated by the storage of alerts and tickets or “cases” (unlimited duration) as well as cold storage of logs. Sekoia Defend Sekoia Exalog
Information (Articles 29 and 30)	The standardization of information on the Sekoia platform (CTI in STIX/TAXII format, SIGMA detection rules, CACAO playbooks, etc.) makes it easier to report incidents and share voluntary information on cyber threats promoted by the directive. Sekoia Intelligence Sekoia Defend

About Sekoia

Sekoia is the European agentic cybersecurity company building the Cyber Operations Platform for the AI era. Unifying cyber threat intelligence, detection and response, exposure management, and agentic AI, Sekoia is rebuilding cybersecurity from the ground up. Through the Autonomous SOC, machines investigate at scale while security teams govern operations with clarity and control. Fully open and agnostic by design, the platform empowers organizations to achieve true strategic and tech autonomy. From SMEs supported by MSSPs to Fortune 2000 enterprises, Sekoia makes advanced defense accessible to all. www.sekoia.com



GET IN TOUCH

Act from clarity

Talk to our team about where you stand on NIS2 — and what to build next.

sekoia.com

trust.sekoia.com · Security & compliance portal