

NIS2 Directive (EU) 2022/2555

NIS2 establishes mandatory cybersecurity and incident-reporting requirements to strengthen resilience across essential and important EU organizations.



What it is

The EU NIS2 Directive is a European Union cybersecurity regulation that establishes measures to ensure a high common level of network and information security across essential and important entities within the EU. Its primary purpose is to strengthen cyber resilience, reduce risks, and improve the response to cyber incidents throughout critical sectors.

Issued by the European Parliament and the Council of the European Union, NIS2 applies to a broad range of operators, including energy, transport, healthcare, digital infrastructure, and public administration. Organizations falling under its scope are required to implement risk management measures, report significant incidents, and comply with oversight obligations covering cybersecurity controls, supply chain security, and governance structures.

At a glance

PUBLISHER European Union Agency for Cybersecurity (ENISA)	TYPE Regulation	VERSION Directive (EU) 2022/2555
EFFECTIVE January 16, 2023	DOMAIN Cybersecurity	FAMILY Other
REGION European Union	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: <https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/network-and-information-systems-directive-2-nis2>

Why it matters

- **Strengthen cybersecurity governance** Foster accountable management structures, ensuring senior leadership oversees and supports information security policies and processes.
- **Improve risk management capabilities** Support ongoing assessment and mitigation of cyber risks through systematic identification of threats and vulnerabilities within critical sectors.
- **Enhance incident reporting and response** Require organizations to promptly detect, report, and respond to cyber incidents, reducing potential impacts on business operations.
- **Support regulatory compliance** Enable organizations to meet evolving EU legal obligations, minimizing regulatory penalties and legal exposure related to cybersecurity incidents.

How SmartSuite supports NIS2 (EU 2022/2555)

Cyber Risk Governance and Ownership Track leadership accountability, policies, and reporting across covered entities.	Risk Management Control Library Organize required measures across prevention, detection, response, and resilience.	Incident Reporting Readiness Manage classification, escalation, and reporting steps with documented evidence.
Supply Chain and Third-Party Oversight Track vendor risks, contracts, monitoring, and contingency planning.	Testing, Exercises, and Improvements Schedule tests and exercises, capture results, and track corrective actions.	Compliance and Readiness Reporting Report status, open gaps, and evidence coverage for leadership and regulators.

Common framework mappings

Official resources

NIS2 Directive Official Text Defines the legislative framework and cybersecurity obligations for essential entities in the EU. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555	NIS2 Guidance by ENISA Provides implementation guidance and best practices for compliance with the NIS2 Directive. enisa.europa.eu/publications/guidelines-for-sectors-govrnis
Video Guide: Introduction to NIS2 Outlines key aspects and impacts of the NIS2 Directive for European organizations. enisa.europa.eu/events/webinar-nis2-direct-access	NIS2 FAQ by ENISA Answers frequently asked questions regarding the NIS2 Directive. enisa.europa.eu/publications/faqs-about-nis2

Frequently asked questions

What is the EU NIS2 Directive used for?

The EU NIS2 Directive is designed to strengthen cybersecurity resilience by setting minimum security and incident reporting requirements for essential and important entities operating within the European Union. Its primary goal is to reduce cyber risks and improve response to incidents in critical sectors such as energy, healthcare, transport, and digital infrastructure.

Is compliance with the EU NIS2 Directive mandatory?

Yes, compliance with NIS2 is mandatory for organizations classified as essential or important entities according to the directive's criteria. Non-compliance can lead to supervisory actions and significant penalties under EU law.

Who does the EU NIS2 Directive apply to?

NIS2 applies to a wide range of organizations, including but not limited to operators in energy, transport, banking, healthcare, digital infrastructure, public administration, and specific digital service providers. Both public and private entities that provide critical services or operate critical infrastructure are within its scope.

What key requirements and controls are mandated by the EU NIS2 Directive?

The directive requires organizations to implement appropriate technical and organizational security measures, conduct regular risk assessments, ensure supply chain security, maintain incident detection and response capabilities, and fulfill prompt notification of significant cybersecurity incidents to national authorities.

How is the EU NIS2 Directive implemented in an organization?

Implementation involves embedding risk management into governance, performing security risk assessments, deploying security controls, ensuring third-party risk management, and developing robust incident response and notification procedures. Organizations must also document controls and remediation steps to demonstrate compliance during regulatory inspections.

How does the EU NIS2 Directive relate to other cybersecurity frameworks?

NIS2 aligns with international standards such as ISO/IEC 27001, and organizations often map its requirements to existing controls within other frameworks. Integrating NIS2 with broader cybersecurity, risk management, and compliance programs supports a unified approach and reduces duplication of effort.

What are the ongoing compliance requirements for the EU NIS2 Directive?

Ongoing compliance requires maintaining up-to-date risk assessments, regularly testing and enhancing cybersecurity controls, monitoring supply-chain dependencies, ensuring timely incident reporting, and undergoing periodic internal and external audits. Compliance teams must stay current with supervisory expectations and evolving regulatory guidance.

How would SmartSuite support the EU NIS2 Directive?

SmartSuite helps manage NIS2 compliance by providing mapped control libraries, risk registers, and policy governance workflows tailored to the directive's requirements. It supports evidence collection, incident and remediation tracking, audit readiness, and real-time reporting dashboards, enabling streamlined oversight and preparation for regulatory inspections.

License included / downloadable: Yes The NIS2 Directive is European Union legislation and is publicly available through official EU regulatory publications.

Full framework page and mappings: smartsuite.com/frameworks/eu-nis2-directive-network-and-information-security-directive-eu-2022-2555