



IN FORCE ACROSS THE EU

NIS2 CYBERSECURITY DIRECTIVE



INTRODUCTION

In an increasingly interconnected and digital world, protecting critical infrastructure and essential services against cyber threats has become a paramount concern for governments, businesses, and individuals. To strengthen cybersecurity across the European Union, the EU adopted the NIS2 Directive, and it is now national law across most of the bloc.

The NIS2 Directive (the Network and Information Systems Directive) is a comprehensive framework designed to strengthen the EU's resilience against cyber incidents. Building on the original NIS Directive of 2016, NIS2 addresses emerging threats, adapts to evolving technologies, and fosters closer collaboration between public and private entities.

Its main objective is harmonized, robust cybersecurity governance across member states, protecting critical infrastructure sectors and digital service providers, and raising the level of readiness and incident response that safeguards the availability, integrity, and confidentiality of vital networks and systems.

In short, NIS2 Directive tightens security requirements in the EU by:

- Extending its scope to more sectors and entities
- Introducing the concept of “management bodies” (corporate accountability)
- Streamlining and standardizing reporting requirements
- Introducing control and monitoring measures
- Harmonizing and strengthening sanctions across all member states

NIS2 was published in the Official Journal (L333) on 27 December 2022 and entered into force on 16 January 2023. The deadline for member states to transpose it into national law was 17 October 2024. That deadline has passed, and NIS2 is now law across most of the EU. In Germany it applies through the amended BSI Act (the NIS2UmsuCG), in force since 6 December 2025 with no transition period, so the obligations apply today.

NIS2 Directive: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

IS MY COMPANY AFFECTED BY NIS2?

The NIS2 Directive distinguishes between essential and important entities. The main difference between the two is that “important entities” are subject to lower fines and reactive supervision by the authorities, as opposed to proactive supervision, which is reserved for “essential entities”.

There will no longer be different minimum thresholds in the EU, but instead, applicability will be determined according to “uniform criteria”. Medium and large companies are to be covered by regulation:

MEDIUM

50–250 employees
10–50 million euros in sales
< 43 million euros in balance sheet

LARGE

> 250 employees
> 50 million euros in sales
> 43 million euros in balance sheet

This significantly expands the number of entities that need to comply with NIS2 in the EU, including Germany.

NIS2 clarifies and strengthens the fines provided for in the law for non-compliance:

- Cybersecurity risk-management measures (Article 21)
- Reporting obligations (Article 23)

Article 34(4) of the NIS2 Directive provides for fines in the event of non-compliance with these obligations. These fines vary depending on whether the entity is essential or important:

- For essential entities, administrative fines of a maximum of at least EUR 10,000,000 or of a maximum of at least 2% of the total worldwide annual turnover
- For important entities, administrative fines of a maximum of at least EUR 7,000,000 or of a maximum of at least 1.4% of the total worldwide annual turnover.

National laws can go beyond the directive's minimum. Germany's BSIG, for example, brings roughly 29,500 organizations into scope across 18 sectors, codifies personal liability for managing directors and boards, and sets fines of up to EUR 10 million or 2% of global annual turnover. Always check the national law where you operate, not only the directive text.

IMPORTANT NOTE:

The authorities will not tell you if this guideline applies. Your company or institution must evaluate itself against the criteria, including sector elements and size considerations. An organization that is 'important' but holds a significant market share in its sector may even be treated as an essential entity based on its size.

CHECK WHETHER NIS2 APPLIES TO YOUR COMPANY

You are considered an **Essential Entity** if both of the following criteria apply:

1. YOUR COMPANY MEETS THESE CRITERIA

- > 250 employees
- > 50 million euros in sales
- > 43 million euros in balance sheet

None of these apply? →

Look at Important Entities.

2. YOUR COMPANY OPERATES IN ONE OF THESE SECTORS:

ENERGY

TRANSPORT

BANKING

FINANCIAL MARKET INFRASTRUCTURE

HEALTH

DRINKING WATER

WASTE WATER

DIGITAL INFRASTRUCTURE

SPACE

ICT SERVICE MANAGEMENT

PUBLIC ADMINISTRATION



You are considered an **Important Entity** if both of the following criteria apply:

1. YOUR COMPANY MEETS THESE CRITERIA

50–250 employees

10–50 million euros in sales

< 43 million euros in balance sheet

None of these apply? →

Look at Essential Entities.

2. YOUR COMPANY OPERATES IN ONE OF THESE SECTORS:

WASTE MANAGEMENT

MANUFACTURING

PRODUCTION/PROCESSING/DISTRIBUTION OF FOOD

POSTAL & COURIER SERVICES

RESEARCH

MANUFACTURE/DISTRIBUTION OF CHEMICALS

DIGITAL PROVIDERS

**DON'T OPERATE IN ANY OF THE SECTORS ABOVE?
NIS2 DOES NOT APPLY TO YOU.**

(Detailed sector lists below.)

NIS2 FOR SUPPLIERS TO IMPORTANT AND ESSENTIAL ENTITIES

Now that NIS2 is in force, the obligations reach beyond directly regulated entities. Companies that act only as suppliers feel it through their customers. The clearest example is the financial sector.

Banks and insurance companies have always had stringent rules, and the “banking supervisory requirements for information technology” (BAIT) provisions are an integral part of their risk management. For third-party service providers, this can mean that a client must assess their cybersecurity and include the result in the annual financial statements prepared by auditing firms.

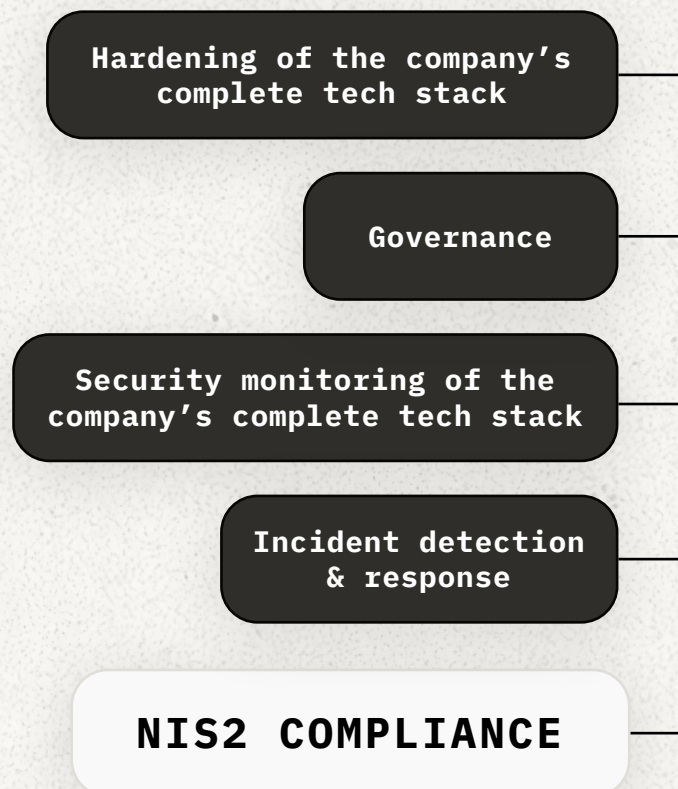
This means that IT service providers and other suppliers must expect to be subjected to supplier audits to examine the robustness of their information security. De facto, this will mean that the supply chain will have to meet the exact requirements that apply to regulated clients.

WHAT IS THE NIS2 DIRECTIVE?

If you are an affected organization, you **must take appropriate action** in areas such as cyber risk management, supply chain security, business continuity management, penetration testing, and incident response, and reporting to the agency and remediation.

NIS2 is an excellent opportunity for Chief Information Security Officers (CISOs) to reinforce their position within the company. Under the directive, **senior management is responsible for managing cybersecurity risks, and violations are punishable by severe penalties.** The CISO is not just an advisor but a guide and leader in decisions. With NIS2, the CISO becomes an executive educator and champion of cybersecurity policies and best practices.

As a CISO, the action plan for NIS2 compliance should focus on 4 main areas:



WHAT ESSENTIAL & IMPORTANT ENTITIES MUST DO

Under the legislation (Article 21), essential and important entities must take at least the following 10 actions:

1. Policies on risk analysis and information system security
2. Incident handling
3. Business continuity, such as backup management and disaster recovery, and crisis management

“Take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on recipients of their services and on other services.”

(NIS2 Article 21)

4. Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
5. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk-management measures
7. Basic cyber hygiene practices and cybersecurity training
8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption
9. Human resources security, access control policies and asset management
10. The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

NIS2 VS ISO 27001:2022

Complying with NIS2 is a multi-year program for many organizations. To make the path clearer, Mondoo maps NIS2 requirements to the ISO/IEC 27001:2022 standard. With the directive now transposed and the Commission's implementing regulation (EU) 2024/2690 setting concrete technical measures for several digital sectors, the requirements are far better defined than they were at adoption, and ISO 27001:2022 remains the most practical lens for gauging how far along you already are.

ISO 27001 provides a framework of best practices for information security policies, procedures, and controls to **minimize the risk** of information security breaches. ISO 27002 focuses on **implementing controls and guidelines**. When aligning NIS2 measures with the ISO 27001:2022 standard, most of the relevant controls come from Annex A, which provides the best control perspective.

Annex A of ISO/IEC 27001:2022 is a section of the standard that lists a set of security controls that organizations can use to demonstrate compliance with ISO/IEC 27001 6.1.3 (Information Security Risk Treatment) and its associated "Statement of Applicability." The Statement of Applicability (SoA) is a mandatory document that lists the Annex A controls that an organization should implement to meet the standard's requirements. Anyone pursuing ISO 27001 certification must complete this step.

NIS2 VS. ISO 27001

NIS2 (Legislations article)	ISO27001:2022
Article 21.2 a) policies on risk analysis and information system security	5.2 Policy 6.1.2 Information security risk assessment 6.1.3 Information security risk treatment 8.2 Information security risk assessment 8.3 Information security risk treatment A.5.1 Policies for information security A.5.12 Classification of information A.5.2 Information security roles and responsibilities A.5.7 Threat intelligence A.5.37 Documented operating procedures
Article 21.2 b) incident handling	A.5.24 Information security incident management planning & preparation A.5.25 Assessment and decision on information security events A.5.26 Response to information security incidents A.5.27 Learning from information security incidents A.5.28 Collection of evidence A.6.8 Information security event reporting A.8.15 Logging; A.8.16 Monitoring activities
Article 21.2 c) business continuity, such as backup management and disaster recovery, and crisis management	A.5.29 Information security during disruption A.5.30 ICT readiness for business continuity A.5.37 Documented operating procedures A.8.13 Information backup A.8.14 Redundancy of information processing facilities A.8.15 Logging A.8.16 Monitoring activities
Article 21.2 d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	A.5.19 Information security in supplier relationships A.5.20 Addressing information security within supplier agreements A.5.21 Managing information security in the ICT supply chain A.5.22 Monitoring, review and change management of supplier services A.5.23 Information security for use of cloud services

NIS2 (Legislations article)	ISO27001:2022
Article 21.2 e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	A.5.37 Documented operating procedures A.8.8 Management of technical vulnerabilities A.8.9 Configuration management A.8.19 Installation of software on operational systems A.8.20 Network security A.8.21 Security of network services
Article 21.2 f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures	9.1 Monitoring, measurement, analysis and evaluation 9.2 Internal audit 9.3 Management review A.5.35 Independent review of information security A.5.36 Compliance with policies, rules & standards for information security
Article 21.2 g) basic cyber hygiene practices and cybersecurity training	7.2 Competence 7.3 Awareness 7.4 Communication A.5.10 Acceptable use of information and other associated assets; A.5.15 Access control A.5.16 Identity management A.6.3 Information security awareness, education and training
Article 21.2 h) policies and procedures regarding the use of cryptography and, where appropriate, encryption	A.8.17 Clock synchronization A.8.24 Use of cryptography
Article 21.2 i) human resources security, access control policies and asset management	A.5.2 Information security roles and responsibilities A.5.3 Segregation of duties A.5.9 Inventory of information and other associated assets A.5.10 Acceptable use of information and other associated assets A.5.11 Return of assets A.5.15 Access control A.5.16 Identity management A.5.17 Authentication information <i>(cont. on next page)</i>

NIS2 (Legislations article)	ISO27001:2022
Article 21.2 i) human resources security, access control policies and asset management (<i>cont.</i>)	A.5.18 Access rights A.6.1 Screening A.6.2 Terms and conditions of employment A.6.3 Information security awareness, education and training A.6.4 Disciplinary process A.6.5 Responsibilities after termination or change of employment A.6.6 Confidentiality or non-disclosure agreements A.6.7 Remote working A.7.7 Clear desk and clear screen A.7.9 Security of assets off-premises A.7.10 Storage media A.7.14 Secure disposal or re-use of equipment A.8.1 User endpoint devices A.8.2 Privileged access rights A.8.3 Information access restriction A.8.4 Access to source code A.8.5 Secure authentication
Article 21.2 j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate	A.5.14 Information transfer A.5.16 Identity management A.5.17 Authentication information A.8.5 Secure authentication
Article 21.3 Member States shall ensure that entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers, including their secure development procedures, and the results of coordinated security risk assessments of critical supply chains under Article 22(1)	A.8.25 Secure development life cycle A.8.26 Application security requirements A.8.27 Secure system architecture and engineering principles A.8.28 Secure coding A.8.29 Security testing in development and acceptance A.8.30 Outsourced development A.8.31 Separation of development, test and production environments A.8.32 Change management A.8.33 Test information
Article 23 Reporting obligations	A.5.14 Information transfer A.6.8 Information security event reporting
Article 24 Use of European cybersecurity certification schemes	A.5.20 Addressing information security within supplier agreements

NIS2: ADDITIONS TO ISO 27001

The ISO 27001 Annex A controls that are not included in the mapping to the NIS2 guideline include:

- **A.5.4** Management responsibilities
- **A.5.5** Contact with authorities
- **A.5.6** Contact with special interest groups
- **A.5.8** Information security in project management
- **A.5.12** Classification of information
- **A.5.13** Labelling of information
- **A.5.31** Legal, statutory, regulatory and contractual requirements
- **A.5.32** Intellectual property rights
- **A.5.33** Protection of records
- **A.5.34** Privacy and protection of personally identifiable information (PII)
- **A.7.1** Physical security perimeters
- **A.7.2** Physical entry
- **A.7.3** Securing offices, rooms and facilities
- **A.7.4** Physical security monitoring
- **A.7.5** Protecting against physical and environmental threats
- **A.7.6** Working in secure areas
- **A.7.8** Equipment siting and protection
- **A.7.11** Supporting utilities
- **A.7.12** Cabling security
- **A.7.13** Equipment maintenance
- **A.8.6** Capacity management
- **A.8.7** Protection against malware
- **A.8.10** Information deletion
- **A.8.11** Data masking
- **A.8.12** Data leakage prevention
- **A.8.17** Clock synchronization
- **A.8.18** Use of privileged utility programs
- **A.8.22** Segregation of networks
- **A.8.23** Web filtering
- **A.8.34** Protection of information systems during audit testing

IN SUMMARY

If you already follow ISO 27001, you're in a good starting position for NIS2. There is only one part that needs to be added to comply with NIS2: incident handling and reporting.

STREAMLINING INCIDENT REPORTING

NIS2 imposes stricter incident response obligations and shorter timeframes than the original NIS Directive. The first step is to create or review your Incident Response Plan, setting out the procedures and policies you will follow so the process is fast and orderly when a reporting obligation is triggered.

The first NIS directive no longer uses the “number of users impacted” threshold. Instead, the NIS2 directive is **based on two distinct concepts for incident response obligations**:

INCIDENTS

Any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems (*Article 6(6)*).

CYBER THREATS

Any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons (*Article 2(8) of the Cybersecurity Act, referred to in Article 6(10) of NIS2*).

Article 23 provides that an incident shall be considered significant if:

1. It has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
2. It has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

In the event of a cyber threat or significant incident, essential and important entities shall notify, without undue delay:

- The competent authorities or the national Computer Security Incident Response Team (CSIRT), while also making sure to report any information enabling determination of any cross-border impact of the incident;
- Where appropriate, the recipients of their services if the incident is likely to affect the provision of that service adversely;
- Where appropriate, those recipients of the threat itself. In a significant cyber threat, measures or remedies that can be taken in response should also be notified.

REPORTING TO CSIRT

When responding to competent authorities or the Computer Security Incident Response Team (CSIRT), you have an obligation to report certain information. This includes any relevant details that are deemed important for the authorities to know.

1. **An initial notification within 24 hours** after becoming aware of the incident, indicating whether it is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
2. **Within 72 hours** of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the previous information and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;
3. Upon the request of a competent authority or a CSIRT, an intermediate report on relevant status updates;
4. A final report not later than **one month** after the submission of the first report, including at least:
 - A detailed description of the incident, its severity and impact;
 - The type of threat or root cause that likely triggered the incident;
 - Applied and ongoing mitigation measures;
 - Where applicable, the cross-border impact of the incident;

5. If the incident is still ongoing at the time of the final report's submission, entities should provide a progress report at that time and a final report within one month of handling the incident.

Each member state runs its own Computer Security Incident Response Team (CSIRT) for incident reporting, and national law designates the competent authorities. In Germany that authority is the BSI, confirmed under the amended BSI Act. France works through ANSSI and Belgium through the CCB.

SECTORS CLASSIFIED AS ESSENTIAL SECTORS IN THE SCOPE OF NIS2

Detailed in Annex I of the NIS2.

Sector	Subsector	Type of Entity
ENERGY	Electricity	Energy supply, Distribution System Operators, Transmission System Operators, Electricity Producers, Electricity Market Operators, and selected participants
	District Heat/ Cooling	Operators for district heating or district cooling
	Oil	Operators of transmission pipelines, Operators of oil production, refining and treatment facilities, storage, and transmission, selected Central oil stock holding entities
	Gas	Suppliers, Distribution system operators, Transmission system operators, Storage system operators, LNG system operators, Natural gas undertakings
TRANSPORT	Air	Air carriers, Airport managing bodies, Air Traffic Control Services Providers (ATC)
	Rail	Infrastructure managers, Railway undertakings

Sector	Subsector	Type of Entity
	Water	Inland, sea and coastal passenger and freight water transport companies, Managing bodies of ports, Operators of vessel traffic services
	Road	Road authorities, Delegated traffic management control regulations, Operators of Intelligent Transport Systems
BANKING		Credit institutions
FINANCIAL MARKET INFRASTRUCTURES		Operators of trading venues, Central counterparties (CCPs)
HEALTH	Pharma, Manufacturing, Laboratories, Services	Healthcare providers, Entities manufacturing medical devices considered critical during a public health emergency, EU reference laboratories, Entities carrying out research and development of medicinal products, Entities manufacturing basic pharmaceutical products and pharmaceutical preparations
DRINKING WATER		Suppliers and distributors of water intended for human consumption, excluding those with the majority of other general activity
WASTE WATER		Undertakings collecting, disposing, or treating urban, domestic, and industrial wastewater when the essential part of the business
SPACE	Infrastructure, Services	Operators of ground-based infrastructure, owned, managed, and operated by Member States or by private parties, that support the provision of space-based services
B2B ICT SERVICES		Managed Services Providers (MSP), Managed Security Services Providers (MSSP)

Sector	Subsector	Type of Entity
DIGITAL INFRASTRUCTURE		Internet Exchange Point providers, DNS service providers, TLD name registries, Cloud computing service providers, Datacenter service providers, Content delivery network providers, Trust service providers, providers of public electronic communications networks, Providers of publicly available electronic communications services
PUBLIC ADMINISTRATION		Public administration entities of central governments and regional level as defined by a Member State in accordance with national law

SECTORS CLASSIFIED AS IMPORTANT SECTORS IN THE SCOPE OF NIS2

Detailed in Annex II of the NIS2.

Sector	Subsector	Type of Entity
POSTAL & COURIER SERVICES		Postal service providers, including providers of courier services
WASTE MANAGEMENT		Undertakings carrying out waste management but excluding those for whom waste management is not their principal economic activity
FOOD PRODUCTION, PROCESSING, DISTRIBUTION		Entities engaged in wholesale distribution, industrial production and processing of any food and drink. Not a food business (e.g. feed, live animals unless for human consumption, plants prior to harvesting)

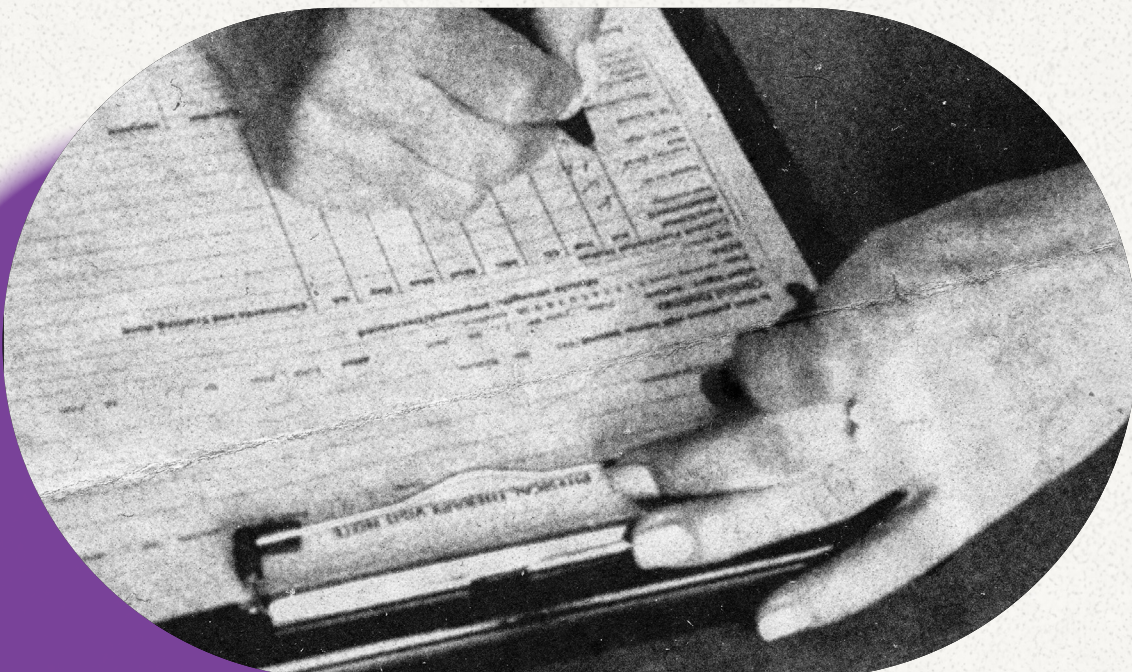
Sector	Subsector	Type of Entity
MANUFACTURING	Medical devices and in vitro diagnostic medical devices	Entities manufacturing medical devices
	Computer, electronic and optical products	Entities that manufacture computers, electronic and optical products, electronic components and boards, communication equipment, consumer electronics, measuring/testing/navigation instruments, watches and clocks, irradiation/electromedical/electrotherapeutic equipment, optical instruments and photographic equipment, magnetic and optical media
	Electrical equipment	Entities that manufacture electrical equipment, motors, generators, transformers and distribution/control apparatus, batteries and accumulators, wiring and wiring devices, fiber optic cables, lighting equipment, domestic appliances, other electrical equipment
	Machinery and equipment n.e.c.	Entities that manufacture general-purpose and special-purpose machinery, engines and turbines, pumps and compressors, taps and valves, bearings and gears, lifting and handling equipment, agricultural and forestry machinery, machine tools, machinery for metallurgy, mining, construction, food/beverage, textile, paper, plastic and rubber, and other machinery n.e.c.
	Motor vehicles, trailers and semi-trailers	Entities that manufacture motor vehicles, trailers and semi-trailers, bodies (coachwork), parts and accessories, electrical and electronic equipment for motor vehicles
	Other transport equipment	Entities that manufacture ships and boats, railway locomotives and rolling stock, air and spacecraft and related machinery, military fighting vehicles, motorcycles, bicycles and invalid carriages, other transport equipment n.e.c.

Sector	Subsector	Type of Entity
DIGITAL PROVIDERS		Providers of online marketplaces, online search engines, and social networking services platforms
RESEARCH		Research organizations

SUMMARY

The NIS2 Cybersecurity Directive updates and broadens EU cybersecurity regulations, aiming to enhance resilience against cyber threats. It extends accountability to top management and imposes significant fines for non-compliance. Additionally, it affects suppliers, requiring evaluations of third-party cybersecurity. Stricter incident response requirements mandate swift reporting to national CSIRTs or competent authorities, emphasizing a proactive approach to cybersecurity.

Organizations should conduct a thorough assessment of their cybersecurity practices and determine their classification under the directive. This self-assessment will help identify areas for improvement and ensure compliance with regulatory requirements.



HOW MONDOO HELPS WITH NIS2 COMPLIANCE

Compliance is a journey, but it doesn't have to be a manual one.

Meeting NIS2 is not about producing longer lists of findings. It is about closing them, continuously, and being able to prove it. **That is where Mondoo changes the equation.**

Mondoo is an agentic exposure management platform that runs one continuous closed loop across your entire estate. It detects vulnerabilities and misconfigurations, prioritizes them by real risk, ships the fix, and verifies the fix held. That loop maps directly onto what Article 21 demands, from vulnerability handling and disclosure through to the ongoing assessment of how effective your security measures actually are.

Mondoo also covers the full path from source code to production. Static code analysis and secret scanning, powered by Mondoo's open-source xgrep across 34+ languages, secure software at the source, while continuous assessment hardens cloud, containers, and the rest of your tech stack. Because NIS2 extends accountability deep into the supply chain, this source-to-close coverage gives both regulated entities and their suppliers the secure-development and third-party assurance evidence the directive requires.

And because Mondoo maps its controls to NIS2 and ISO/IEC 27002:2022 out of the box, compliance shifts from a multi-year manual exercise into continuous, evidence-backed monitoring you can put straight in front of an auditor.

**YOU DON'T JUST FIND THE GAPS.
YOU CLOSE THEM, AND YOU CAN
SHOW YOUR WORK.**

MONDOO.COM