Comprehensive Guide to the NIS 2 Directive

Advisera

Introduction

This white paper is intended for people who are starting to learn about the European Union's NIS 2 Directive, and it presents the basic facts and guidance for this new Directive.

The paper covers the following topics:

- The basics of NIS 2
- Which companies must become compliant
- Main NIS 2 requirements
- Implementation steps
- Required documents
- Reporting obligations
- Performing training and awareness
- Relationship with other frameworks
- Role of the government and transposition to local laws

1. NIS 2 basics

1.1. NIS 2 Directive summary

The “NIS 2 Directive,” or simply “NIS2,” is a European Union directive that specifies cybersecurity requirements that need to be implemented by EU companies that are considered to be critical infrastructure.

Its full name is “Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union,” and it was published on December 14, 2022.

Since NIS 2 is a directive, this means that each EU country will define its own cybersecurity laws based on NIS 2, whereas NIS 2 specifies the minimum level of cybersecurity to be achieved. In practice, this means that companies in some countries will have to comply with the minimum specified in NIS 2, and in other countries they will have to comply with more strict cybersecurity requirements specified in local laws.

NIS 2 has the mark “2” because it replaces the old NIS directive.

1.2. What is the old NIS directive, and how is NIS 2 different?

The old NIS directive (Directive 2016/1148) also specified cybersecurity for critical infrastructure, but it did not manage to introduce the same level of cybersecurity across all Member States, resulting in a fragmented approach.

The new NIS 2 introduces a wider array of industries (sectors) that must be compliant, better cooperation between the Member States, new timelines for reporting incidents, more focus on supply chains, the responsibility on the top management of entities, stricter penalties, etc.

1.3. When does NIS 2 come into effect?

NIS 2 will take effect on October 18, 2024 – this is also the deadline for EU countries to define their own laws and regulations based on NIS 2.

1.4. What does “NIS” stand for?

The full title of the old NIS directive was: “Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.”

Therefore, “NIS” is an abbreviation of “Network and Information Systems.”

1.5. Why is NIS 2 important?

NIS 2 is important because it sets very strict cybersecurity requirements for a large number of companies in the European Union – by some estimates, more than 100,000 companies in the European Union will have to become NIS 2 compliant.

Even though NIS 2 does not apply to as many companies as, e.g., the EU GDPR, it will certainly become a de facto standard for critical infrastructure that other (non-EU) countries will emulate – a very similar scenario has happened already in non-EU countries with privacy regulations that are very similar to the EU GDPR.

1.6. Where can I find the full text of NIS 2?

You can find the official text here: https://eur-lex.europa.eu/eli/dir/2022/2555.

You can also find the full text here, arranged by chapters and articles, and with the ability to search by keyword: NIS 2 Directive Full Text.

1.7. What is the structure of NIS 2?

NIS 2 starts with a preamble where, in 144 points, it explains the background and provides some guidelines for the main part of the Directive. The main part of NIS 2 has 46 articles that are structured in the following chapters:

- Chapter I — General provisions
- Chapter II — Coordinated cybersecurity frameworks
- Chapter III — Cooperation at union and international level
- Chapter IV — Cybersecurity risk-management measures and reporting obligations
- Chapter V — Jurisdiction and registration
- Chapter VI — Information sharing
- Chapter VII — Supervision and enforcement
- Chapter VIII — Delegated and implementing acts
- Chapter IX — Final provisions
- Annex I — Sectors of high criticality
- Annex II — Other critical sectors
- Annex III — Correlation table between NIS 2 and NIS

You can read all the NIS 2 articles here: Full Text of the NIS 2 Directive.

1.8. What are the main cybersecurity requirements of NIS 2?

Surprisingly, only Chapter IV "Cybersecurity risk-management measures and reporting obligations" defines what essential and important entities must do to comply with NIS 2. All the other chapters are not relevant for these companies, because they specify the obligations of the EU countries (Member States), and what government agencies must do to enforce NIS 2.

Chapter IV has the following articles:

- Article 20 - Governance
- Article 21 - Cybersecurity risk-management measures
- Article 22 - Union level coordinated security risk assessments of critical supply chains
- Article 23 - Reporting obligations
- Article 24 - Use of European cybersecurity certification schemes
- Article 25 – Standardisation

2. Which companies must become compliant

The NIS 2 Directive clearly lists all the sectors and subsectors (industries) that need to comply with this European cybersecurity directive. However, there are many exceptions to this list, and the line between essential and important entities is not very easy to understand, so this section clarifies who needs to be compliant, and in what status.

2.1. Criteria that determine which companies must comply with NIS 2

There are three general criteria that define which organizations must comply with NIS 2:

- 1) Location — if they provide services or carry out activities in any country in the European Union (no matter if they are based in the EU or not), and
- 2) Size — if they are categorized as mid-sized or large organizations (see the criteria in the section below), and
- 3) Industry — if they operate in any of the 18 sectors listed in the table below.

However, there are some exceptions to these rules — see the table in the section below for further explanation.

2.2. What are essential and important entities?

“Essential entities” and “important entities” are what NIS 2 calls companies and other organizations that need to comply with NIS 2.

NIS 2 defines *essential entities* as follows:

- Companies that are categorized as large enterprises (see the criteria in the next section) and are in one of the 11 critical sectors (listed in the table below)
- Trust service providers
- DNS service providers
- Public electronic communication networks
- Public administration entities
- Any critical entity according to Critical Entities Resilience (CER) Directive (EU) 2022/2557
- Other entities specified by Member States

Important entities are all other organizations that are not categorized as essential entities, but that fall under the 3 criteria mentioned in the previous section.

2.3. Breakdown of sectors & essential and important entities

Since the above explanation from NIS 2 is a bit confusing, the table below shows which organizations need to comply with NIS 2, and if they are classified as essential or important entities.

For clarification, here’s how the EU classifies companies according to their size:

- *Micro and small organizations* — if they have fewer than 50 employees and less than 10 million euros in annual revenue.

- *Mid-size organizations* — if they have 50 to 250 employees and 10 to 50 million euros in annual revenue.
- *Large organizations* — if they have more than 250 employees and more than 50 million euros in annual revenue.

Sector	Subsector	Type of entity	Micro and small organizations*	Mid-sized organizations	Large organizations
Sectors of high criticality					
1. Energy	(a) Electricity	Electricity undertakings which carry out the function of 'supply'	(NIS 2 compliance not required)	Important entity	Essential entity
		Distribution system operators	(NIS 2 compliance not required)	Important entity	Essential entity
		Transmission system operators	(NIS 2 compliance not required)	Important entity	Essential entity
		Producers	(NIS 2 compliance not required)	Important entity	Essential entity
		Nominated electricity market operators Market participants Operators of a recharging point	(NIS 2 compliance not required)	Important entity	Essential entity
	(b) District heating and cooling	Operators of district heating or district cooling	(NIS 2 compliance not required)	Important entity	Essential entity
	(c) Oil	Operators of oil transmission pipelines	(NIS 2 compliance not required)	Important entity	Essential entity
		Operators of oil production, refining and treatment facilities, storage and transmission	(NIS 2 compliance not required)	Important entity	Essential entity
		Central stockholding entities	(NIS 2 compliance not required)	Important entity	Essential entity
	(d) Gas	Supply undertakings	(NIS 2 compliance not required)	Important entity	Essential entity
		Distribution system operators	(NIS 2 compliance not required)	Important entity	Essential entity
		Transmission system operators	(NIS 2 compliance not required)	Important entity	Essential entity
		Storage system operators	(NIS 2 compliance not required)	Important entity	Essential entity
		LNG system operators	(NIS 2 compliance not required)	Important entity	Essential entity
		Natural gas undertakings	(NIS 2 compliance not required)	Important entity	Essential entity
		Operators of natural gas refining and treatment facilities	(NIS 2 compliance not required)	Important entity	Essential entity
	(e) Hydrogen	Operators of hydrogen production, storage and transmission	(NIS 2 compliance not required)	Important entity	Essential entity

Sector	Subsector	Type of entity	Micro and small organizations*	Mid-sized organizations	Large organizations
2.Transport	(a) Air	Air carriers used for commercial purposes	(NIS 2 compliance not required)	Important entity	Essential entity
		Airport managing bodies, airports, including the core airports, and entities operating ancillary installations contained within airports	(NIS 2 compliance not required)	Important entity	Essential entity
		Traffic management control operators providing air traffic control (ATC) services	(NIS 2 compliance not required)	Important entity	Essential entity
	(b) Rail	Infrastructure managers	(NIS 2 compliance not required)	Important entity	Essential entity
		Railway undertakings, including operators of service facilities	(NIS 2 compliance not required)	Important entity	Essential entity
	(c) Water	Inland, sea and coastal passenger and freight water transport companies, not including the individual vessels operated by those companies	(NIS 2 compliance not required)	Important entity	Essential entity
		Managing bodies of ports, including their port facilities, and entities operating works and equipment contained within ports	(NIS 2 compliance not required)	Important entity	Essential entity
		Operators of vessel traffic services (VTS)	(NIS 2 compliance not required)	Important entity	Essential entity
	(d) Road	Road authorities responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity	(NIS 2 compliance not required)	Important entity	Essential entity
		Operators of Intelligent Transport Systems	(NIS 2 compliance not required)	Important entity	Essential entity
3. Banking	(Subsector not specified)	Credit institutions	(NIS 2 compliance not required)	Important entity	Essential entity
4. Financial market infrastructures	(Subsector not specified)	Operators of trading venues	(NIS 2 compliance not required)	Important entity	Essential entity
		Central counterparties (CCPs)	(NIS 2 compliance not required)	Important entity	Essential entity
5. Health	(Subsector not specified)	Healthcare providers	(NIS 2 compliance not required)	Important entity	Essential entity
		EU reference laboratories	(NIS 2 compliance not required)	Important entity	Essential entity

Sector	Subsector	Type of entity	Micro and small organizations*	Mid-sized organizations	Large organizations
		Entities carrying out research and development activities of medicinal products Entities manufacturing basic pharmaceutical products and pharmaceutical preparations Entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list)	(NIS 2 compliance not required)	Important entity	Essential entity
6. Drinking water	(Subsector not specified)	Suppliers and distributors of water intended for human consumption, excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods	(NIS 2 compliance not required)	Important entity	Essential entity
7. Waste water	(Subsector not specified)	Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water, excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity	(NIS 2 compliance not required)	Important entity	Essential entity
8. Digital infrastructure	(Subsector not specified)	Internet Exchange Point providers	(NIS 2 compliance not required)	Important entity	Essential entity
		DNS service providers, excluding operators of root name servers	Essential entity	Essential entity	Essential entity
		TLD name registries	Essential entity	Essential entity	Essential entity
		Domain name registration services	Important entity	Important entity	Important entity
		Cloud computing service providers	(NIS 2 compliance not required)	Important entity	Essential entity
		Data centre service providers	(NIS 2 compliance not required)	Important entity	Essential entity
		Content delivery network providers	(NIS 2 compliance not required)	Important entity	Essential entity
		Trust service providers	Essential entity	Essential entity	Essential entity
		Providers of public electronic communications networks	Important entity	Essential entity	Essential entity
		Providers of publicly available electronic communications services	Important entity	Essential entity	Essential entity
9. ICT service management (business-to-business)	(Subsector not specified)	Managed service providers Managed security service providers	(NIS 2 compliance not required)	Important entity	Essential entity

Sector	Subsector	Type of entity	Micro and small organizations*	Mid-sized organizations	Large organizations
10. Public administration	(Subsector not specified)	Public administration entities of central governments as defined by a Member State in accordance with national law	Essential entity	Essential entity	Essential entity
		Public administration entities at regional level as defined by a Member State in accordance with national law	Essential entity	Essential entity	Essential entity
		Public administration entities at local level	(if a Member State decides)	(if a Member State decides)	(if a Member State decides)
11. Space	(Subsector not specified)	Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks	(NIS 2 compliance not required)	Important entity	Essential entity
Other critical sectors					
1. Postal and courier services	(Subsector not specified)	Postal service providers, including providers of courier services	(NIS 2 compliance not required)	Important entity	Important entity
2. Waste management	(Subsector not specified)	Undertakings carrying out waste management, excluding undertakings for whom waste management is not their principal economic activity	(NIS 2 compliance not required)	Important entity	Important entity
3. Manufacture, production and distribution of chemicals	(Subsector not specified)	Undertakings carrying out the manufacture of substances and the distribution of substances or mixtures, and undertakings carrying out the production of articles from substances or mixtures	(NIS 2 compliance not required)	Important entity	Important entity
4. Production, processing and distribution of food	(Subsector not specified)	Food businesses which are engaged in wholesale distribution and industrial production and processing	(NIS 2 compliance not required)	Important entity	Important entity
5. Manufacturing	(a) Manufacture of medical devices and in vitro diagnostic medical devices	Entities manufacturing medical devices, and entities manufacturing in vitro diagnostic medical devices with the exception of entities manufacturing medical devices	(NIS 2 compliance not required)	Important entity	Important entity
	(b) Manufacture of computer, electronic and optical products	Undertakings carrying out any of the economic activities	(NIS 2 compliance not required)	Important entity	Important entity
	(c) Manufacture of electrical equipment	Undertakings carrying out any of the economic activities	(NIS 2 compliance not required)	Important entity	Important entity

Sector	Subsector	Type of entity	Micro and small organizations*	Mid-sized organizations	Large organizations
	(d) Manufacture of machinery and equipment n.e.c.	Undertakings carrying out any of the economic activities	(NIS 2 compliance not required)	Important entity	Important entity
	(e) Manufacture of motor vehicles, trailers and semi-trailers	Undertakings carrying out any of the economic activities	(NIS 2 compliance not required)	Important entity	Important entity
	(f) Manufacture of other transport equipment	Undertakings carrying out any of the economic activities	(NIS 2 compliance not required)	Important entity	Important entity
6. Digital providers	(Subsector not specified)	Providers of online marketplaces	(NIS 2 compliance not required)	Important entity	Important entity
		Providers of online search engines	(NIS 2 compliance not required)	Important entity	Important entity
		Providers of social networking services platforms	(NIS 2 compliance not required)	Important entity	Important entity
7. Research	(Subsector not specified)	Research organisations	(NIS 2 compliance not required)	Important entity	Important entity
		Education institutions, in particular where they carry out critical research activities	(if a Member State decides)	(if a Member State decides)	(if a Member State decides)

*Micro and small organizations also need to be compliant with NIS 2 in the following cases:

- If, according to NIS 2 Article 2 paragraph 2:
  - "(b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;
  - (c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;
  - (d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;
  - (e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;"
- If a Member State has defined that entity as a "critical entity" according to Critical Entities Resilience (CER) Directive (EU) 2022/2557

2.4. What is different for essential and important entities in NIS 2?

Here are the most important differences in how NIS 2 treats essential and important entities:

- Article 32 specifies stricter supervisory and enforcement measures for essential entities than those specified in Article 33 for important entities.

- Article 34 specifies higher fines for essential entities:
  - For essential entities – the fines are up to 10 million euro or 2% of the total annual turnover.
  - For important entities – the fines are up to 7 million euro or 1.4% of the total annual turnover.

Back to main page

Backup Policy

Customize document

Step 3: Backup procedure

Who is in charge of performing the backup?

System administrator

Which technology are you using for backup?

AWS

Preview of related section

Backup procedure

3. Main NIS 2 requirements

Out of 46 articles in the NIS 2 Directive, only articles 20 to 25 are really relevant for companies (i.e., essential and important entities) that must become compliant with NIS 2; most of the other articles specify the requirements for government bodies that regulate cybersecurity.

These most important requirements are placed in Chapter IV, and they revolve around two main topics: cybersecurity risk management and reporting obligations. Besides Chapter IV, there are only a few requirements relevant for essential and important entities.

So, here are the most important NIS 2 requirements you should be aware of:

3.1. Responsibilities of senior management

According to Article 20, the top management of essential and important entities:

- must approve cybersecurity measures that need to be implemented in the company,
- must oversee their implementation, and
- can be held liable if cybersecurity is not implemented properly.

Articles 32 and 33 further emphasizes the liability of the legal representatives of essential entities and important entities.

3.2. Importance of training

According to Article 20, members of top management must go through cybersecurity training, and they must enable their employees to attend such training on a regular basis.

NIS 2 requires such training to cover identification of risks, assessment of cybersecurity practices, and how these cybersecurity measures help the company provide its services.

3.3. Risk-based approach to cybersecurity

Article 21 requires cybersecurity measures to be appropriate for the related risks; when assessing the risks, NIS 2 requires companies to take into account the following:

- exposure to risks
- company size
- likelihood of occurrence of incidents and their severity
- societal and economic impacts of incidents

3.4. Cybersecurity as a mixture of technical, operational, and organizational measures

Article 21 requires companies to “take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems … and to prevent or minimise the impact of incidents on recipients of their services and on other services."

Further, Article 21 requires an all-hazards approach, which basically means that companies have to prepare for a wide range of potential threats.

Finally, Article 21 specifies a range of cybersecurity documents and measures, which are listed in the section below.

3.5. Supply chain security

Article 21 requires companies to pay special attention to risks related to direct suppliers and service providers, in particular:

- Vulnerabilities specific to each direct supplier and service provider
- The overall quality of products and cybersecurity practices of suppliers and service providers
- Secure development procedures of suppliers and service providers

3.6. Reporting of significant incidents

Article 23 requires companies to report any significant incidents to computer security incident response teams (CSIRTs) and to the users of their services.

See the section below to learn about the reports that must be sent.

3.7. Using certified IT products and services

NIS 2 does not require essential and important entities to get certified. However, the NIS 2 Directive allows for EU countries (Member States) or the EU Commission to require those entities to use IT products or services that are certified. At the time of writing this article, there are no requirements for using certified IT products or services, but there is a high chance that this will become mandatory.

Those IT products and services will need to be certified according to the European cybersecurity certification scheme.

3.8. Fines and liability

For companies that are not NIS 2 compliant, the fines are as follows:

- For essential entities – up to 10 million euros or 2% of the total annual turnover.
- For important entities – up to 7 million euros or 1.4% of the total annual turnover.

It is important to note that Article 20 requires the top management of essential and important entities to approve the cybersecurity risk management measures and oversee their implementation, and it specifies that top management can be held liable if cybersecurity is not compliant with Article 21.

4. Implementation steps for cybersecurity risk management measures

Complying with complex regulations like the NIS 2 Directive is never easy, but if you have a clear plan for how to do it, this whole project will become more straightforward. Below you will see a best practice on which steps to follow to achieve full compliance with NIS 2 Chapter IV “Cybersecurity risk-management measures and reporting obligations” — the steps focus on this chapter because it presents key NIS 2 requirements that companies (i.e., essential and important entities) need to be compliant with.

4.1. Step 1) Obtain senior management support

You might think that, since NIS 2 is mandatory, complying with this regulation will go smoothly with or without senior management commitment. Unfortunately, the reality is different — if the top management does not actively support such a project, it will be slow, underfunded, and blocked at every possible step.

So, even though NIS 2 is mandatory, you still have to convince your executives that this is something worth focusing on.

4.2. Step 2) Set up project management

NIS 2 is too complex to just give it to your, e.g., IT administrator, hoping that everything will turn out fine. First of all, you cannot expect someone without formal authority to succeed with such a big project, and second – you need to have a clear idea of the implementation steps, milestones, main outcomes, responsibilities, etc.

In other words, a project approach is necessary if you want to succeed.

4.3. Step 3) Perform initial training

NIS 2 places a big emphasis on performing security training, and it makes sense to perform initial training very early in the project.

This way, everyone involved will have a much better picture of what NIS 2 is, what needs to be done, why it is needed, etc. — and you will launch your project much more easily.

See the section below on how to start with NIS 2 training.

4.4. Step 4) Write a top-level Policy on Information System Security

Even though NIS 2 does not specifically require a top-level document that would define the direction for cybersecurity, such a document is a best practice according to international standards because of the following fact: if you don’t know where you are going, you will likely get lost.

This is why such a top-level document is needed – it clearly shows what needs to be achieved with cybersecurity, what the main roles and responsibilities are, and how the success will be measured.

4.5. Step 5) Define the Risk Management Methodology

Risk management is usually the most complex step in the compliance process, and, on top of this, NIS 2 has some specific requirements for how this risk management needs to be done.

To make sure that your company is compliant with NIS 2, and to make sure everyone in the company understands how risks need to be managed, you have to create a document that specifies clear rules – this is done through the Risk Management Methodology document.

4.6. Step 6) Perform risk assessment and treatment

During the risk assessment, you have to find out what could jeopardize your information systems – this is usually done by listing assets and related threats and vulnerabilities; further, you have to find out how big those risks are by assessing likelihood and severity (impact).

After you have the list of risks, you have to figure out how to treat (i.e., mitigate) the highest risks – for most of them, you will implement the cybersecurity measures defined in Article 21. In this way, you have cybersecurity that is based on a thorough analysis, rather than implementing various measures without knowing why.

4.7. Step 7) Write and approve the Risk Treatment Plan

Once you have a complete idea of which risks you have and how to treat them, you will need to create a concrete plan for how to implement cybersecurity measures – and, even more importantly, to get the approval of senior management for such a plan.

The Risk Treatment Plan is in fact an implementation plan, and it typically includes a list of all cybersecurity measures (i.e., activities, processes, and technologies) that need to be implemented, together with information on who is in charge, what the deadlines are, etc.

4.8. Step 8) Implement cybersecurity measures

Of course, the key NIS 2 requirement is to implement various cybersecurity measures. In practice, this means that you will have to introduce new security processes, activities, and, in some cases, new technology, all based on the results of the risk assessment.

In any case, you will have to write various cybersecurity policies and procedures to set clear rules for those new processes, activities, and technologies.

See the section below about the required documents to learn which cybersecurity measures are needed, and which documents to use.

4.9. Step 9) Set up supply chain security

NIS 2 has recognized that an increasing number of security incidents are related to breaches with suppliers – it requires paying close attention to relationships with suppliers and service providers, which includes assessment of their vulnerabilities, and studying their software development procedures.

This is done through a formal risk assessment of suppliers, selecting only reliable suppliers to work with, including security clauses in agreements with them, and monitoring their security posture.

4.10.Step 10) Set up the assessment of cybersecurity effectiveness

NIS 2 requires the senior management to oversee the implementation of cybersecurity measures – the best practice is to do this in three ways: (1) by continuously measuring and monitoring cybersecurity to be able to spot any deviations, (2) by introducing periodic internal audits to discover nonconformities, and (3) by introducing periodic management review to have a formal session for reviewing all facts related to cybersecurity.

To set up those activities, you have to write a few key documents: Measurement Methodology, Internal Audit Procedure, and Management Review Procedure.

4.11. Step 11) Set up incident reporting

One of the key NIS 2 requirements is to notify the CSIRT (or competent authority), and the recipients of services, about significant incidents.

Entities need to submit several types of reports to the CSIRT: an early warning, an incident notification, an intermediate report, a final report, and a progress report.

See the section below to learn more about reporting obligations.

4.12.Step 12) Set up continual cybersecurity training

NIS 2 is very specific about setting up cybersecurity for all employees, including the senior management. The challenge here is how to select the right topics, and what form of training to choose in order to get the right knowledge transfer without spending too much time or money.

See the section below to learn about potential approaches to resolve these dilemmas.

4.13.Step 13) Periodic internal audit

It is true that the internal audit is not mentioned in NIS 2; however, ISO 27001 and other international standards suggest the internal audit as the best practice for senior management to be able to oversee the implementation of cybersecurity measures.

Without identifying nonconformities during the internal audit, the senior management would never have a complete picture of the state of cybersecurity, which could lead to incidents and liability.

4.14.Step 14) Periodic management review

A management review is a formal meeting at which the senior management needs to receive all relevant information about cybersecurity (e.g., Measurement Report, Internal Audit Report, etc.) in order to make key decisions about cybersecurity.

During the management review, the senior management could raise corrective actions, change key roles and responsibilities, set new security objectives, define the security budget, etc.

4.15. Step 15) Execute corrective actions

Corrective actions are a systematic way to resolve nonconformities – during their implementation, the cause of a nonconformity is formally analyzed, and the activities to eliminate this cause are defined and executed.

In other words, the purpose of corrective actions is to make sure that similar nonconformities do not happen again.

5. Required documents for NIS 2

If your company needs to comply with the NIS 2 Directive, you'll have to write lots of new documents to cover cybersecurity and reporting requirements. This section presents all the documents that companies need to write according to NIS 2 Chapter IV "Cybersecurity risk-management measures and reporting obligations" — the reason why the focus is only on this chapter is that it is the only one that specifies what essential and important entities need to do to comply with this Directive.

5.1. List of required documents and records

The table below shows NIS 2 requirements, the relevant articles from Chapter IV of this Directive, and the best practice of documenting those requirements.

What must be documented	NIS 2 / CIR article	Usually documented through
Management bodies must approve the cybersecurity risk-management measures	Article 20, paragraph 1 CIR 2024/2690 Annex point 2.1	Risk Treatment Plan
Management bodies must oversee the implementation of cybersecurity risk-management measures	Article 20, paragraph 1 CIR 2024/2690 Annex point 7	Measurement Report + Internal Audit Report + Management Review Minutes
Members of the management bodies are required to follow training, and must offer similar training to their employees on a regular basis	Article 20, paragraph 2 CIR 2024/2690 Annex point 8	Training and Awareness Plan
Entities must take appropriate and proportionate technical, operational, and organizational measures to manage the risks	Article 21, paragraph 1 CIR 2024/2690 Annex point 2.1	Risk Treatment Table + Risk Treatment Plan + various policies and procedures mentioned below
When assessing the proportionality of measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact	Article 21, paragraph 1 CIR 2024/2690 Annex point 2.1	Risk Assessment Methodology + Risk Assessment Table
Policy on risk analysis	Article 21, paragraph 2, point (a) CIR 2024/2690 Annex point 2.1	Risk Assessment Methodology
Policy on information system security	Article 21, paragraph 2, point (a) CIR 2024/2690 Annex point 1.1	Policy on Information System Security

What must be documented	NIS 2 / CIR article	Usually documented through
Incident handling	Article 21, paragraph 2, point (b) CIR 2024/2690 Articles 3 to 14 and Annex points 3.1, 3.3, 3.4, 3.5, 3.6, and 4.3.3	Incident Handling Policy + Incident Log
Business continuity	Article 21, paragraph 2, point (c) CIR 2024/2690 Annex point 4.1	Business Continuity Plan
Backup management	Article 21, paragraph 2, point (c) CIR 2024/2690 Annex point 4.2	Backup Policy
Disaster recovery	Article 21, paragraph 2, point (c) CIR 2024/2690 Annex point 4.1	Disaster Recovery Plan
Crisis management	Article 21, paragraph 2, point (c) CIR 2024/2690 Annex point 4.3	Crisis Management Plan
Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	Article 21, paragraph 2, point (d) CIR 2024/2690 Annex point 5	Supplier Security Policy + Security Clauses for Suppliers and Partners + Confidentiality Statement
Security in network and information systems acquisition, development and maintenance	Article 21, paragraph 2, point (e) CIR 2024/2690 Annex points 6.1, 6.2, and 6.5	Policy for the Acquisition, Development, and Maintenance of ICT Systems + Specification of Acquisition, Development, and Maintenance Requirements of ICT System
Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	Article 21, paragraph 2, point (f) CIR 2024/2690 Annex point 7	Measurement Methodology + Measurement Report + Internal Audit Procedure + Internal Audit Checklist + Internal Audit Report + Management Review Procedure
Basic cyber hygiene practices	Article 21, paragraph 2, point (g) CIR 2024/2690 Annex point 8.1	IT Security Policy

What must be documented	NIS 2 / CIR article	Usually documented through
Cybersecurity training	Article 21, paragraph 2, point (g) CIR 2024/2690 Annex point 8	Training and Awareness Plan
Policies and procedures regarding the use of cryptography and encryption	Article 21, paragraph 2, point (h) CIR 2024/2690 Annex point 9	Policy on Encryption and Cryptographic Controls
Human resources security	Article 21, paragraph 2, point (i) CIR 2024/2690 Annex point 10	Security Policy for Human Resources
Access control policies	Article 21, paragraph 2, point (i) CIR 2024/2690 Annex point 11	Access Control Policy
Asset management	Article 21, paragraph 2, point (i) CIR 2024/2690 Annex point 12	Asset Management Procedure + IT Asset Register
The use of multi-factor authentication or continuous authentication solutions	Article 21, paragraph 2, point (j) CIR 2024/2690 Annex points 11.6 and 11.7	Authentication Policy
Secured voice, video and text communications	Article 21, paragraph 2, point (j)	Information Transfer Policy + Secure Communication Policy
Secured emergency communication systems within the entity	Article 21, paragraph 2, point (j)	Secure Communication Policy
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 and service providers, including their secure development procedures	Article 21, paragraph 3 CIR 2024/2690 Annex point 5.1	Supplier Security Policy + Risk Assessment and Treatment Report
Take appropriate and proportionate corrective measures	Article 21, paragraph 4 CIR 2024/2690 Annex points 2.3.3, 3.6, and 4.1.4	Procedure for Corrective Action + Corrective Action Form
Notify CSIRT or competent authority of significant incident	Article 23, paragraph 1 CIR 2024/2690 Annex point 3.5	Significant Incident Notification for CSIRT/Competent Authority

What must be documented	NIS 2 / CIR article	Usually documented through
Notify the recipients of services of significant incidents that are likely to adversely affect the provision of those services	Article 23, paragraph 1 CIR 2024/2690 Annex point 3.3	Significant Incident Notification for Recipients of Services
Communicate to the recipients of services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat; also inform those recipients of the significant cyber threat itself	Article 23, paragraph 2 CIR 2024/2690 Annex point 3.3	Significant Incident Notification for Recipients of Services
An early warning that indicates whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact	Article 23, paragraph 4, point (a) CIR 2024/2690 Annex point 3.5	Significant Incident Early Warning
An incident notification that indicates an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise	Article 23, paragraph 4, point (b) CIR 2024/2690 Annex point 3.5	Significant Incident Notification for CSIRT/Competent Authority
An intermediate report on relevant status updates	Article 23, paragraph 4, point (c) CIR 2024/2690 Annex point 3.5	Significant Incident Intermediate Report
A final report not later than one month after the submission of the incident notification	Article 23, paragraph 4, point (d) CIR 2024/2690 Annex point 3.5	Significant Incident Final Report
A progress report - in the event of an ongoing incident at the time of the submission of the Final Report	Article 23, paragraph 4, point (e) CIR 2024/2690 Annex point 3.5	Significant Incident Progress Report

5.2. Cybersecurity documents required by CIR 2024/2690

Besides the required documents listed above, if a company is a digital critical infrastructure company (any of the following: DNS service provider; TLD name registry; cloud computing service provider; data center service provider; content delivery network provider; managed service provider; managed security service provider; trust service provider; or the provider of an online marketplace, an online search engine, or a social networking services platform), the following documents are also mandatory:

- Acceptance of Residual Risks – document used to formally accept the risks that are left after the cybersecurity measures are applied.
- Physical Security Policy — defines security rules for data centers, archives, and other areas that need special protection.

- Information Classification Policy — provides clear rules on how to classify documents and other information, and how to protect those assets according to classification level.
- Network Security Policy – defines basic rules for ensuring the security of networks against intrusions and data misuse.
- Vulnerability and Patch Management Procedure – aims to ensure the correct and secure application of software code changes or updates, known as patches, to fix security or functionality problems, add new capabilities, or improve the performance of software and ICT equipment.
- ICT Change Management Procedure — defines rules on how to perform changes in production systems, in order to decrease security risks.
- Business Impact Analysis Methodology – defines the methodology and process for assessing the impacts of disruptive activities and determines continuity and recovery priorities, objectives, and targets.
- Business Continuity Strategy – defines which options and solutions a company will utilize to ensure that all conditions for the resumption of business activities in the case of disaster or other disruptive incident are met.
- Recovery Time Objectives for Activities – determines recovery time objectives for each activity, taking into account dependencies on other activities.
- Activity Recovery Strategy for an individual activity – defines the recovery strategy for an individual activity, and solutions to implement that strategy.
- Disruptive Incident Response Plan – defines solutions for direct response to the occurrence of various types of incidents.
- List of Business Continuity Sites – specifies all provided alternative sites.
- Key Contacts – specifies the contact information for all key contacts within the company.
- Exercising and Testing Plan – determines the frequency and methods of testing in order to assess the feasibility of measures and solutions for business continuity management, and to establish necessary corrective actions.
- Exercising and Testing Report – specifies the results of exercising and testing, appropriate corrective actions that must be initiated, and other recommendations for improvement.
- Directory of Suppliers and Service Providers – registry of the company's direct suppliers and service providers.
- Minor Incident Response Procedure – ensures a timely, consistent, and systematic response to incidents that are not considered disruptive.
- Post Incident Review Form – used to assess all the relevant aspects of handling an incident

5.3. Common cybersecurity documents that are not required by NIS 2

Besides the required documents listed above, it is also recommended to write the following documents:

- Mobile Device and Work from Home Policy — specifies the rules for using laptops, smartphones, and other devices outside of company premises.
- Bring Your Own Device (BYOD) Policy — specifies security aspects if employees are using their private devices for work.
- Disposal and Destruction Policy — specifies how to dispose of devices and media, in order to delete all sensitive data and avoid breaking intellectual property rights.

- Clear Desk and Clear Screen Policy — defines rules for each employee on how to protect his/her workspace.
- Security Procedures for IT Department — provides security operating procedures for activities that are not covered in other documents.

Who is in charge of performing the backup?
System administrator

Which technology are you using for backup?
AWS

6. How to report incidents

The NIS 2 Directive only specifies reporting obligations in Article 23, but this article is quite lengthy and quite demanding. So, which incidents do you need to report, to whom do you need to report them, and how do you need to do so?

6.1. What is a significant incident according to NIS 2?

According to NIS 2, an incident "means an 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."

NIS 2 requires only significant incidents to be reported – it defines a significant incident as "any incident that has a significant impact on the provision" of the services that essential and important entities provide, if:

- "a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
- (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage."

Recital (101) in the preamble of NIS 2 says "Indicators such as the extent to which the functioning of the service is affected, the duration of an incident or the number of affected recipients of services could play an important role in identifying whether the operational disruption of the service is severe."

Other than this, no guideline has been published on what a "severe financial loss" would mean, or what "considerable material or non-material damage" would be.

Both essential and important entities need to report significant incidents, while there are no requirements to report other types of incidents.

6.2. To whom are incidents reported?

NIS 2 requires essential and important entities to notify the following parties of significant incidents:

- The computer security incident response team (CSIRT) or a competent authority (these authorities are designated by Member States to be responsible for cybersecurity and for the supervisory tasks).
- Recipients of services from essential or important entities that are potentially affected by the significant incident.

6.3. How are significant incidents reported?

Article 23 requires companies to report significant incidents in the following ways:

NIS 2 requirement	Relevant NIS 2 article	When to report	What to report	Suggested document name
A notification (for the recipients of services that are potentially affected by a significant cyber threat)	Article 23, paragraph 2	Without undue delay	Any measures or remedies that those recipients are able to take in response to that threat; also inform those recipients of the significant cyber threat itself	Significant Incident Notification for Recipients of Services
An early warning (for CSIRT or competent authority)	Article 23, paragraph 4, point (a)	Without undue delay and, in any event, within 24 hours of becoming aware of the significant incident	Indicates whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact	Significant Incident Early Warning
An incident notification (for CSIRT or competent authority)	Article 23, paragraph 4, point (b)	Without undue delay and, in any event, within 72 hours of becoming aware of the significant incident	Indicates an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise	Significant Incident Notification for CSIRT/competent authority
An intermediate report (for CSIRT or competent authority)	Article 23, paragraph 4, point (c)	Upon the request of a CSIRT or the competent authority	Relevant status updates	Significant Incident Intermediate Report
A final report (for CSIRT or competent authority)	Article 23, paragraph 4, point (d)	Not later than one month after the submission of the incident notification	(i) A detailed description of the incident, including its severity and impact; (ii) the type of threat or root cause that is likely to have triggered the incident; (iii) applied and ongoing mitigation measures; (iv) where applicable, the cross-border impact of the incident	Significant Incident Final Report
A progress report (for CSIRT or competent authority)	Article 23, paragraph 4, point (e)	In the event of an ongoing incident	(not specified)	Significant Incident Progress Report

7. Performing training and awareness according to NIS 2

The NIS 2 Directive states very clearly that all employees, including the senior management, need to go through cybersecurity training. So, where should you start – which topics should be covered, and how should the whole process be organized?

7.1. Which topics to cover in NIS 2 cybersecurity training and awareness

In Chapter IV Cybersecurity risk-management measures and reporting obligations, NIS 2 specifies various activities and security measures that need to be performed.

The best approach to defining topics for cybersecurity training and awareness is to cover each of these activities and measures. However, not all of these topics will be appropriate for everyone in the company — therefore, you will see below that the topics are separated according to the target audience.

7.1.1. Topics for all employees (including the mid-level and senior management)

- The basics of the NIS 2 Directive (cover all relevant articles)
- Basic cyber hygiene practices (Article 21 paragraph 2 point g)
- Incident handling (Article 21 paragraph 2 point b)
- Backup (Article 21 paragraph 2 point c)
- Business continuity (Article 21 paragraph 2 point c)
- The use of multi-factor authentication and continuous authentication solutions (Article 21 paragraph 2 point j)

7.1.2. Topics for IT employees and security managers

- Policy on information system security (Article 21 paragraph 2 point a)
- Disaster recovery (Article 21 paragraph 2 point c)
- Security in network and information systems acquisition, development, and maintenance (Article 21 paragraph 2 point e)
- Policies and procedures regarding the use of cryptography and encryption (Article 21 paragraph 2 point h)
- Access control (Article 21 paragraph 2 point i)
- Asset management (Article 21 paragraph 2 point i)
- Secured voice, video, and text communications (Article 21 paragraph 2 point j)
- Secured emergency communication systems (Article 21 paragraph 2 point j)

7.1.3. Topics specific to security managers

- Steps for NIS 2 compliance (relevant articles in Chapter IV)
- How is NIS 2 related to ISO 27001? (Preamble recital (79), Article 21 paragraph 1, Article 25)
- How is NIS 2 related to DORA? (Preamble recital (28))
- How is NIS 2 related to CER? (Article 2 paragraph 3, Article 3 paragraph 1 point f)
- How is NIS 2 related to the EU GDPR? (Preamble recital (121), Article 35)
- Certification of IT products and services (Article 24)
- Government bodies defined in NIS 2 (several articles)

- Organizing regular cybersecurity trainings for different levels of employees in a company (Article 20 paragraph 2; Article 21 paragraph 2 point g)
- How to perform risk assessment and treatment according to NIS 2 (Article 21 paragraph 1)
- Assessing vulnerabilities and quality of suppliers (Article 21 paragraph 3)
- Human resources security (Article 21 paragraph 2 point i)
- Assessing the effectiveness of cybersecurity risk management measures (Article 21 paragraph 2 point f)
- Taking corrective measures (Article 21 paragraph 4)

7.1.4. Topics for top management and security managers

- What are the essential and important entities that must comply with NIS 2? (Article 3)
- Main cybersecurity requirements of NIS 2 (Article 21)
- Approving and overseeing cybersecurity risk management measures (Article 20 paragraph 1)
- Crisis management (Article 21 paragraph 2 point c)
- Supply chain security (Article 21 paragraph 2 point d)
- Reporting obligations (Article 23)
- NIS 2 fines and liabilities (Article 20 paragraph 1; Article 32 paragraph 6; Article 34)
- Cybersecurity legislation by EU countries (Article 41)

7.2. The process of setting up NIS 2 training

Overall, the process of setting up cybersecurity training that is compliant with NIS 2 should follow these steps:

1. Assess the risks in the company — this is the basis for writing security documents, and for finding out what to focus on in cybersecurity training.
2. Define cybersecurity policies and procedures — this way, cybersecurity roles and responsibilities become clear.
3. Define the target groups for training within the company — groups of employees with different cybersecurity roles.
4. Define topics for the training – based on risks, roles, and responsibilities – that will differ for various target groups.
5. Define how often the training will be delivered, how it will be measured, and who will be in charge.

7.3. Options for delivering training on a regular basis

There are several options for delivering NIS 2 cybersecurity training:

7.3.1. a) Instructor-led in-classroom training

- Pros:
  - Training can be adapted according to the needs of the company
  - Higher engagement
- Cons:
  - Probably the most expensive

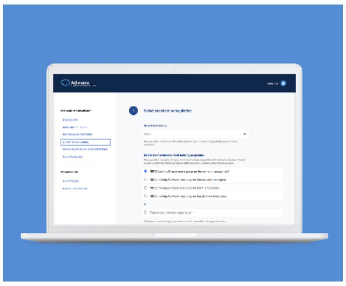
  - Cannot be delivered very often
  - Hard to deliver separate training for different target groups

7.3.2. b) Instructor-led online training

- Pros:
  - Training can be adapted according to the needs of the company
- Cons:
  - Lower engagement

7.3.3. c) Pre-recorded online training delivered via learning management system (LMS)

- Pros:
  - Easy tracking of attendance and test results
  - Employees can watch videos at their convenience
  - The most budget-friendly option
- Cons:
  - Attendees cannot ask questions to the instructor directly



8. Relationship with other frameworks

8.1. How is NIS 2 related to ISO 27001?

NIS 2 does not require the implementation of ISO 27001; however, it does mention the ISO/IEC 27000 series in the preamble as a way to implement cybersecurity risk management measures, and the main part of NIS 2 encourages the use of international standards.

When comparing NIS 2 with ISO 27001 more closely, it becomes clear that ISO 27001 provides an excellent framework for complying with the cybersecurity risk management measures required by NIS 2. ISO 27001 provides a clear guide on how to define the risk management process, how to combine technical implementation with training and other HR issues, how to involve the top management, etc.

8.2. What is the difference between NIS 2 and the EU GDPR?

The full title of the EU GDPR is “Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).”

Even though both NIS 2 and the GDPR both focus on protection of data, they are quite different:

	NIS 2	EU GDPR
Type	Directive (companies comply with local legislation that is published)	Regulation (directly applicable to companies)
Applies to	Organizations that are considered essential and important entities	Any organization that processes personal data
Protection	Cybersecurity measures are applied to all data within the company	Cybersecurity measures apply to personal data only; there is also a legal aspect of protection of personal data
Effective from	October 18, 2024	May 25, 2018

8.3. What is the difference between NIS 2 and DORA?

The full title of DORA is “Regulation (EU) 2022/2554 on digital operational resilience for the financial sector.”

Although NIS 2 and DORA were both published on the same day (December 27, 2022), there are big differences between them:

	NIS 2	DORA
Type	Directive (companies comply with local legislation that is published)	Regulation (directly applicable to financial institutions)
Applies to	Organizations that are considered essential and important entities	Financial institutions
Protection	Emphasis on cybersecurity measures	Besides cybersecurity measures, the emphasis is also on overall resilience
Effective from	October 18, 2024	January 17, 2025

8.4. What is the difference between NIS 2 and the Critical Entities Resilience Directive (CER)

The full title of CER is "Directive (EU) 2022/2557 on the resilience of critical entities."

Although NIS 2 and CER (as well as DORA) were published on the same day (December 27, 2022), they have a different focus:

	NIS 2	CER
Type	Directive (companies comply with local legislation that is published)	Directive (companies comply with local legislation that is published)
Applies to	Organizations that are considered essential and important entities	Organizations that are considered critical according to Member State decision
Protection	Emphasis on cybersecurity measures	Emphasis on resilience and business continuity
Effective from	October 18, 2024	October 18, 2024; however, critical entities need to become compliant within 10 months from the day they are designated as critical

9. Role of the government; transposition to local laws

9.1. Which government bodies are defined in NIS 2?

Here is what NIS 2 defines:

- “Member States” are countries that are members of the European Union – they must publish their own cybersecurity laws and regulations based on NIS 2.
- “Competent authorities” are designated by Member States to supervise the essential and important entities that must be compliant with NIS 2 and local cybersecurity laws.
- “Single points of contact” are established by Member States to enable cross-border cooperation between authorities.
- “Cyber crisis management authorities” are competent authorities, designated by Member States, which are responsible for the management of large-scale cybersecurity incidents and crises.
- “Computer security incident response teams” (CSIRTs) are designated by Member States in order to handle incidents in accordance with defined processes.
- The “European cyber crisis liaison organisation network” (EU-CyCLONe) supports the coordinated management of large-scale cybersecurity incidents and crises.
- The “Cooperation Group” facilitates strategic cooperation and the exchange of information among Member States.
- The “European Union Agency for Cybersecurity” (ENISA) establishes a vulnerability database, creates a biennial report on the state of cybersecurity in the Union, maintains a registry of entities with special status, draws up guidelines regarding the technical areas and existing standards, etc.

9.2. Which laws did EU countries publish based on NIS 2? (Transposition of NIS 2)

EU countries (Member States) must publish local laws and regulations related to the NIS 2 Directive by October 17, 2024 – this process of adopting local legislation based on an EU directive is called “transposition.”

As of the date of updating this white paper (February 2025), the following Member States have transposed NIS 2 into their local legislation:

- Overview of Croatia’s NIS2 Cybersecurity Regulation
- What are additional requirements of Croatia’s Cybersecurity Act when compared to NIS 2?
- Overview of Lithuania’s Decision on Cybersecurity Requirements
- What are the additional requirements of Lithuania’s Cybersecurity Act when compared to NIS2?
- Overview of the Italian NIS2 law and comparison with the EU NIS2 Directive
- What are the additional requirements of Belgium’s cybersecurity law when compared to NIS 2?
- Overview of Latvia’s Cybersecurity Law and Comparison with the NIS2 Directive

9.3. NIS 2 certification

NIS 2 does not require essential and important entities to get certified.

However, Member States (or the EU commission) may require those entities to use particular IT products or services that are certified in accordance with the European cybersecurity certification scheme according to the Cybersecurity Act (EU Regulation 2019/881).

Sources:

- NIS 2 Directive
- Series of NIS 2 articles on Advisera.com

Author:

Dejan Kosutic

Leading expert on cybersecurity & information security and the author of several books, articles, webinars, and courses. As a premier expert, Dejan founded Advisera to help small and medium businesses obtain the resources they need to become compliant with EU regulations and ISO standards. He believes that making complex frameworks easy to understand and simple to use creates a competitive advantage for Advisera's clients, and that AI technology is crucial for achieving this.

As an ISO 27001 and NIS 2 expert, Dejan helps companies find the best way to compliance by eliminating overhead and adapting the implementation to their size and industry specifics.

Advisera Expert Solutions Ltd
for electronic business and business consulting
www.advisera.com

Our offices

US Office
1178 Broadway, 3rd Floor #3829
New York NY 10001
United States

EU Office
Zavizanska 12
10000 Zagreb
Croatia, European Union

EMAIL:
support@advisera.com

Advisera