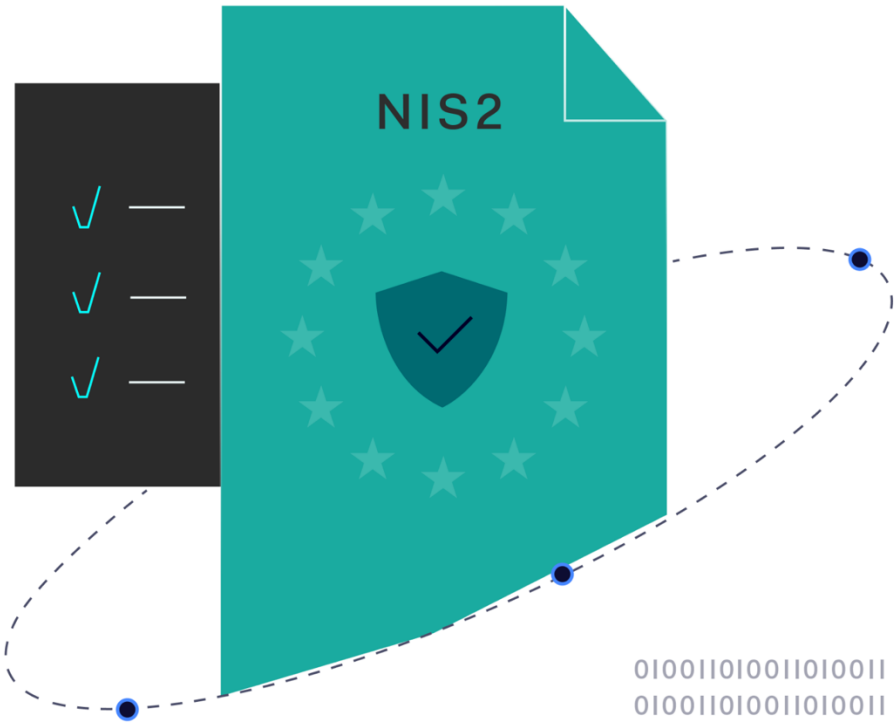
NIS 2
Compliant.*org*

Comprehensive guide to the NIS 2 directive

www.NIS2*Compliant.org* | V 2.0, Updated in June 24, 2024



Abstract

In this white paper, we provide an overview of the NIS2 Directive and its impact on Information Technology (IT) and Operational Technology (OT) security for organizations within the scope of the revised NIS Directive.

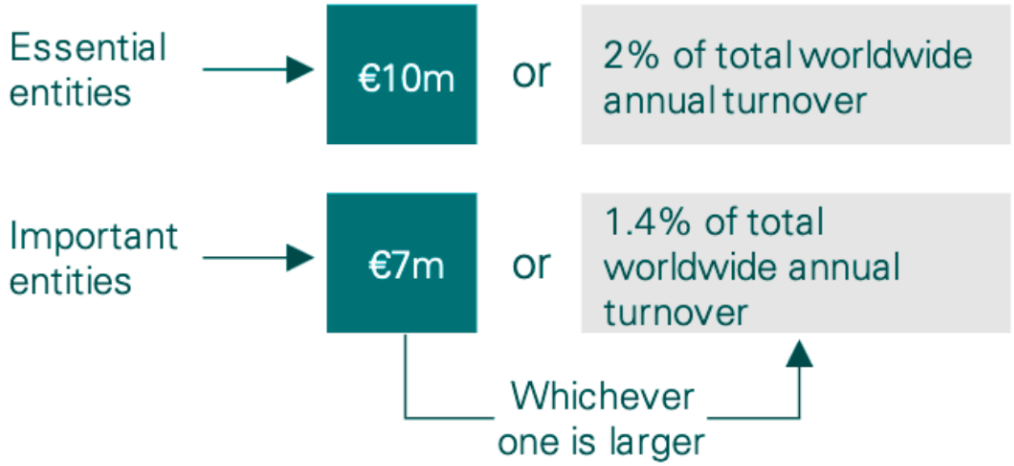
We will share NIS2Compliant.org's view on NIS2, compare NIS2 to related internationally recognized frameworks, and discuss the implications for organizations with an IT and OT convergence use case. We explain how NIS2Compliant.org supports businesses to take control and improve their cybersecurity governance, communication, and strategy across the three organizational lines, while achieving compliance with the new requirements and reducing cyber risks.

This paper provides a detailed overview to navigate the challenges of the NIS2 Directive and work towards strengthening cybersecurity capabilities.

Revision of the Initial NIS Directive (2016)

Sixteen key sectors fall within the broadened scope of the revised NIS2 Directive. The European Union has signed the NIS2 Directive as part of a more proactive approach to addressing cybersecurity issues across the region. As the world becomes more connected, organizations find their IT and OT infrastructures increasingly integrated, heightening the potential for physical cybersecurity incidents. Consequently, the NIS2 Directive underscores the EU's commitment to prioritizing cybersecurity.

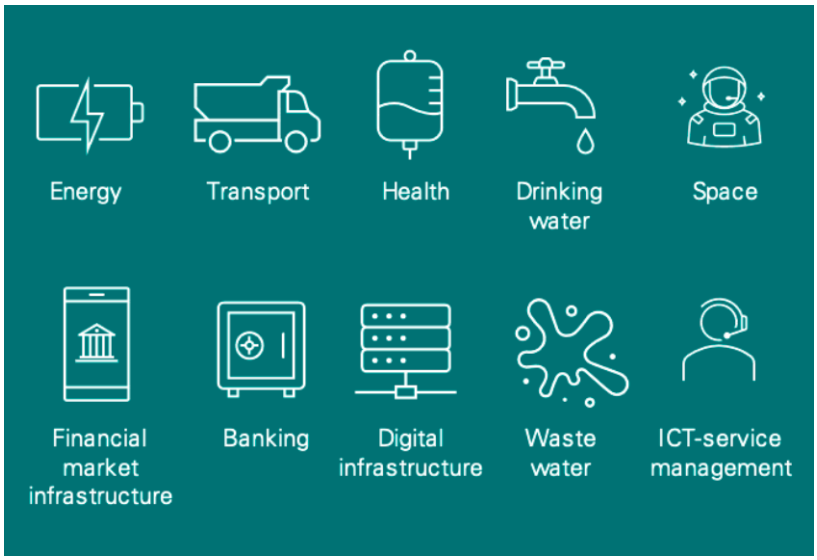
The NIS2 Directive primarily targets organizations essential to the supply chain of critical infrastructure. With the detailed requirements of the NIS2 Directive still more than a year away from release, it is understandable that essential and important entities may be uncertain about their next steps. Based on current knowledge, it is crucial for critical organizations to enhance their cybersecurity governance and risk management measures and prepare for the new reporting obligations. These organizations must utilize internationally recognized frameworks, such as the IEC 62443 series for OT security, to meet the necessary compliance requirements.



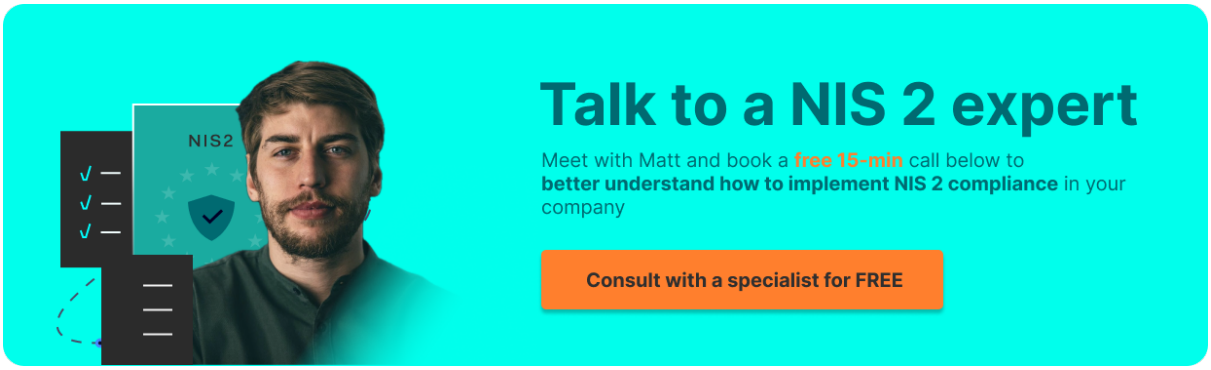
The NIS2 Directive is significantly more mandatory compared to the initial NIS Directive. The EU will now impose financial penalties, similar to those under GDPR legislation, on organizations that fail to comply within the given timeframe. Additionally, the controls specified in the detailed requirements will include strict technical measures to ensure secure operations, extending beyond IT within the business.

Moreover, there will be potential repercussions for C-level executives in organizations that fail to comply with the NIS2 Directive, including possible restrictions on positions they hold within executive boards.

The compliance landscape is becoming increasingly complex for European businesses that must maintain various control frameworks to ensure compliance across all business lines. To manage this complexity, the approach of "test once, comply to many" can help organizations navigate the increasingly challenging regulatory environment.



The sectors mentioned above will be under the most stringent supervision of the NIS2 Directive. However, other organizations may also fall within its scope (page 7). If your organization is affected by the NIS2 Directive, our detailed approach (page 17) provides a comprehensive guide on how to respond to the legislation. This will help companies achieve compliance in a timely and effective manner.



Does your organization fall within the scope of NIS 2?

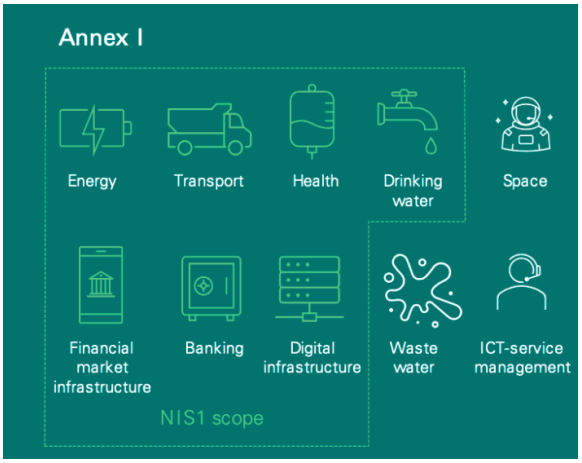
In 2016, the initial NIS Directive made reference to 7 key sectors. Since then, the EU has expanded their view of the sectors that are considered critical to a safe, efficient and effective society. Under the NIS2 Directive the scope has therefore broadened significantly with an expansion of 9 additional sectors. **Sixteen key sectors** in total now fall within the broadened scope of the revised NIS2 Directive.

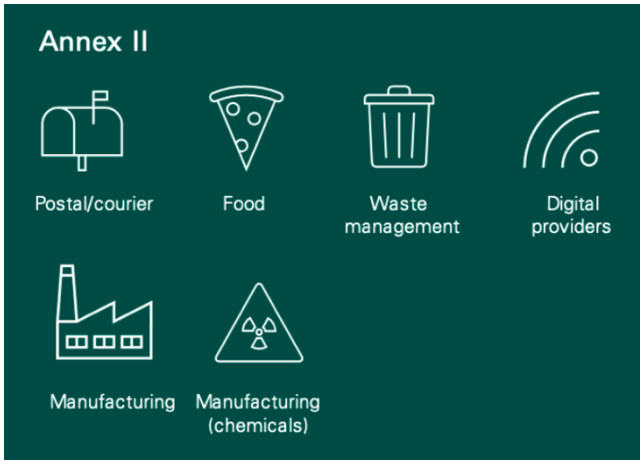
Questions to ask

- Does our company provide a critical service or essential function directly to end clients or as a key supplier that could impact public safety or economic stability, such as those listed here?
- Does our company operate in a sector covered by the NIS2 Directive, such as those listed here?
- Is our company based outside the EU but offering critical services within the EU? If so, this Directive also applies to you!
- Does the lex specialist principle apply? (Where a sector-specific EU legal act provides equivalent cybersecurity requirements or incident notification obligations, these sector-specific acts take precedence - e.g., DORA, PSD2.)

Critical sectors: Annex I & Annex II

The NIS2 scope is covered by two annexes. The Directive applies to both public and private entities referred to in **Annex I or II**, as depicted below. **Annex I** lists the sectors of high criticality, which can be either an **Essential** or an **Important** entity depending on the total annual revenue and size of the organisation.





Annex II provides the other critical sectors set out by the EU, which will only fall into the Important Entity category.

Criteria that determine which companies must comply with NIS 2

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

• **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

• **Size** — if they are categorized as mid-sized or large organizations (see the criteria in the section below), and

• **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.

Essential and Important entities

NIS2 categorizes entities within its scope into two groups: 'essential' and 'important'. The primary distinction is that a disruption of services by entities in the essential group would have serious consequences for the country's society as a whole.

Both groups must comply with the same security measures. However, entities in the essential category are under proactive supervision, while important entities are

monitored only after a non-compliance incident is reported. Organizations must promptly determine if they fall within the scope and whether they are classified as an essential or important entity.

“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.

Classification of Sectors: Essential and Important Entities

Given the potentially confusing explanation of NIS2 above, the table below clarifies which organizations need to comply with NIS2 and whether they are classified as essential or important entities.

To further clarify, 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.

Legend:

Exceptions

Sector	Subsector	Type of Sector	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'	Not required	Important entity	Essential entity
		Distribution system operators	Not required	Important entity	Essential entity
		Transmission system operators	Not required	Important entity	Essential entity
		Producers	Not required	Important entity	Essential entity

		Nominated electricity market operators. Market participants. Operators of a recharging point	Not required	Important entity	Essential entity
	(b) District heating and cooling	Operators of district heating or district cooling	Not required	Important entity	Essential entity
	(c) Oil	Operators of oil transmission pipelines	Not required	Important entity	Essential entity
		Operators of oil production, refining and treatment facilities, storage and transmission	Not required	Important entity	Essential entity
		Central stockholding entities	Not required	Important entity	Essential entity
	(d) Cas	Supply undertakings	Not required	Important entity	Essential entity
		Distribution system operators	Not required	Important entity	Essential entity
		Transmission system operators	Not required	Important entity	Essential entity
		Storage system operators	Not required	Important entity	Essential entity
		LNG system operators	Not required	Important entity	Essential entity
		Natural gas undertakings	Not required	Important entity	Essential entity
		Operators of natural gas refining and treatment facilities	Not required	Important entity	Essential entity
	(e) Hydrogen	Operators of hydrogen production, storage and transmission	Not required	Important entity	Essential entity
2.Transport	(a) Air	Air carriers used for commercial purposes	Not required	Important entity	Essential entity
		Airport managing bodies, airports, including the core airports, and entities operating ancillary installations contained within airports	Not required	Important entity	Essential entity
		Traffic management control operators providing air traffic control (ATC) services	Not required	Important entity	Essential entity
	(b) Rail	Infrastructure managers	Not required	Important entity	Essential entity
		Railway undertakings, including operators of service facilities	Not required	Important entity	Essential entity

	(c) Water	In land, sea and coastal passenger and freight water transport companies, not including the individual vessels operated by those companies	Not required	Important entity	Essential entity
		Managing bodies of ports, including their port facilities, and entities operating works and equipment contained within ports	Not required	Important entity	Essential entity
		Operators of vessel traffic services (VTS)	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	Not required	Important entity	Essential entity
		Operators of Intelligent Transport Systems	Not required	Important entity	Essential entity
3. Banking	Subsector not specified	Credit institutions	Not required	Important entity	Essential entity
4. Financial market infrastructure	(Subsector not specified)	Operators of trading venues	Not required	Important entity	Essential entity
		Central counterparties (CCPs)	Not required	Important entity	Essential entity
5. Health	(Subsector not specified)	Healthcare providers	Not required	Important entity	Essential entity
		EU reference laboratories	Not required	Important entity	Essential entity
		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)	Not required	Important entity	Essential entity

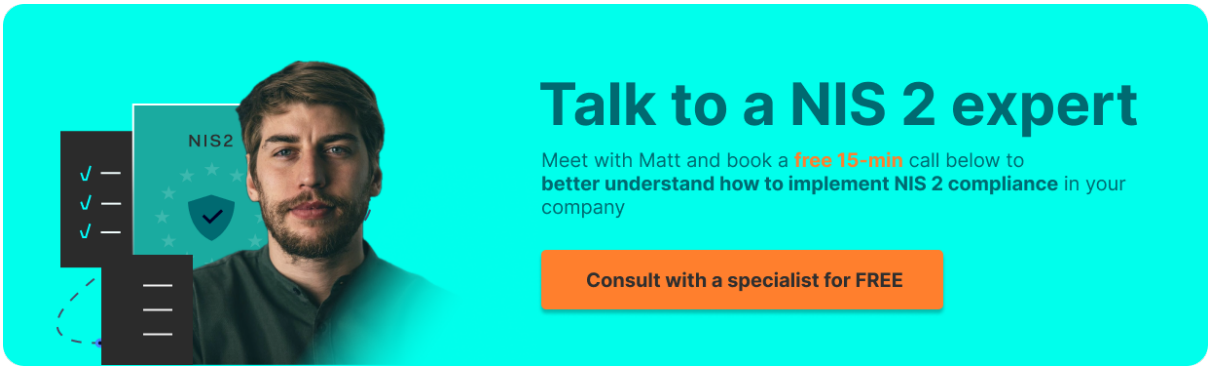
6. Drinking water	(Subsector not specified)	Suppliers and distributors of water intended for human consumption, excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods	Not required	Important entity	Essential entity
7. Wastewater	(Subsector not specified)	Undertakings collecting, disposing overtreating urban wastewater, domestic wastewater 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	Not required	Important entity	Essential entity
B. Digital infrastructure	(Subsector not specified)	Internet Exchange Point Providers	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	Not required	Important entity	Essential entity
		Data center service providers	Not required	Important entity	Essential entity
		Content delivery network providers	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 and Managed security service providers	Not required	Important entity	Essential entity
10. Public administration	(Subsector not specified)	Public administration entities of central governments as defined by a Member State in accordance with national law	Not required	Essential entity	Essential entity
		Public administration entities at regional level as defined by a Member State in accordance with national law	Not required	Essential entity	Essential entity
		Public administration entities at local level	(if a Member State decides)	Member State decides)	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	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	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	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	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	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 except for entities manufacturing medical devices	Not required	Important entity	Important entity
	(b) Manufacture of computer, electronic and optical products	Undertakings carrying out any of the economic activities	Not required	Important entity	Important entity
	(c) Manufacture of electrical equipment	Undertakings carrying out any of the economic activities	Not required	Important entity	Important entity

	(d) Manufacture of machinery and equipment n.e.c.	Undertakings carrying out any of the economic activities	Not required	Important entity	Important entity
	(e) Manufacture of motor vehicles, trailers and semi- trailers	Undertakings carrying out any of the economic activities	Not required	Important entity	Important entity
	(f) Manufacture of other transport equipment	Undertakings carrying out any of the economic activities	Not required	Important entity	Important entity
6. Digital providers	(Subsector not specified)	Providers of online marketplaces	Not required	Important entity	Important entity
		Providers of online search engines	Not required	Important entity	Important entity
		Providers of social networking services platforms	Not required	Important entity	Important entity
7.Research	(Subsector not specified)	Research organizations	Not required	Important entity	Important entity
		Education institutions, 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



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.

Main NIS2 Requirements

Out of the 46 articles in the NIS2 Directive, only articles 20 to 25 are particularly relevant for companies classified as essential and important entities that need to comply with NIS2. The majority of the other articles outline the requirements for government bodies responsible for regulating cybersecurity.
The most critical requirements are found in Chapter IV, focusing on two main areas: cybersecurity risk management and reporting obligations. Apart from Chapter IV, there are only a few other requirements pertinent to essential and important entities.
Here are the key NIS2 requirements you should be aware of:

Responsibilities of Senior Management

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

- Must approve the cybersecurity measures that need to be implemented in the company.
- Must oversee the implementation of these measures.
- Can be held liable if cybersecurity is not properly implemented.

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

Importance of Training

According to Article 20, members of top management must undergo cybersecurity training and enable their employees to attend regular training sessions. NIS2 requires this training to cover risk identification, cybersecurity practice assessment, and how these measures help the company provide its services.

Risk-Based Approach to Cybersecurity

Article 21 mandates that cybersecurity measures must be appropriate for the related risks. When assessing risks, NIS2 requires companies to consider:

- Exposure to risks
- Company size
- Likelihood and severity of incidents
- Societal and economic impacts of incidents

Cybersecurity as a Mixture of Technical, Operational, and Organizational Measures

Article 21 requires companies to "take appropriate and proportionate technical, operational, and organizational measures to manage the risks posed to the security of network and information systems ... and to prevent or minimize the impact of incidents on recipients of their services and on other services." This all-hazards approach means companies must prepare for a wide range of potential threats.

Supply Chain Security

Article 21 also requires companies to pay special attention to risks related to direct suppliers and service providers, focusing on:

- Vulnerabilities specific to each supplier and service provider
- Overall quality of products and cybersecurity practices
- Secure development procedures

Reporting of Significant Incidents

Article 23 mandates that companies report any significant incidents to computer security incident response teams (CSIRTs) and their service users. See the section below for required reports.

Using Certified IT Products and Services

NIS2 does not require essential and important entities to get certified. However, the Directive allows EU Member States or the EU Commission to mandate the use of certified IT products or services. While this is not currently a requirement, it may become mandatory in the future, requiring certification according to the European cybersecurity certification scheme.

Fines and Liability

For non-compliance with NIS2:

- **Essential entities** may face fines up to **10 million euros** or **2% of total annual turnover.**
- **Important entities** may face fines up to **7 million euros** or **1.4% of total annual turnover.**

It's important to note that Article 20 requires the top management of essential and important entities to approve and oversee the implementation of cybersecurity risk management measures. **Top management can be held liable if cybersecurity measures are not compliant with Article 21.**

15 steps to compliance

Complying with complex regulations like the NIS2 Directive can be challenging, but having a clear plan can simplify the process. Below is a best practice guide to achieving full compliance with NIS2 Chapter IV "Cybersecurity Risk-Management Measures and Reporting Obligations," which outlines key requirements for essential and important entities.

Step 1: Obtain Senior Management Support

Despite NIS2 being mandatory, active support from senior management is crucial. Without their commitment, the project can be slow, underfunded, and obstructed. Convincing executives of the importance of focusing on NIS2 compliance is essential.

Step 2: Set Up Project Management

NIS2 compliance is too complex to be handled by an individual without formal authority, like an IT administrator. A structured project management approach is necessary, with clear implementation steps, milestones, outcomes, and responsibilities.

Step 3: Perform Initial Training

NIS2 emphasizes security training. Early in the project, provide training to ensure everyone understands NIS2, what needs to be done, and why. This will facilitate a smoother project launch.

Step 4: Write a Top-Level Policy on Information System Security

Although not specifically required by NIS2, a top-level policy document is a best practice. It defines cybersecurity goals, roles, responsibilities, and success metrics, ensuring clear direction.

Step 5: Define the Risk Management Methodology

Risk management is complex, and NIS2 has specific requirements. A Risk Management Methodology document is needed to ensure compliance and clarify how risks should be managed within the company.

Step 6: Perform Risk Assessment and Treatment

Identify potential threats to information systems by listing assets and related threats and vulnerabilities. Assess the likelihood and severity of these risks. Then, develop strategies to mitigate the highest risks, implementing cybersecurity measures defined in Article 21.

Step 7: Write and Approve the Risk Treatment Plan

Create a detailed plan to implement cybersecurity measures, and obtain senior management approval. The Risk Treatment Plan should list all cybersecurity activities, processes, and technologies, along with responsible parties and deadlines.

Step 8: Implement Cybersecurity Measures

Implement necessary cybersecurity measures based on risk assessment results. This may involve new processes, activities, technologies, and creating various cybersecurity policies and procedures.

Step 9: Set Up Supply Chain Security

Address security risks related to suppliers by assessing their vulnerabilities, evaluating their software development procedures, and including security clauses in agreements. Monitor their security posture regularly.

Step 10: Set Up the Assessment of Cybersecurity Effectiveness

Senior management must oversee cybersecurity implementation. Best practices include continuous monitoring, periodic internal audits, and management reviews to identify nonconformities and ensure effective cybersecurity measures.

Step 11: Set Up Incident Reporting

One of the key NIS2 requirements is to notify the CSIRT (or competent authority) and service recipients about significant incidents. Prepare to submit early warnings, incident notifications, intermediate reports, final reports, and progress reports.

Step 12: Set Up Continual Cybersecurity Training

NIS2 requires regular cybersecurity training for all employees, including senior management. Choose appropriate training topics and formats to ensure effective knowledge transfer without excessive costs.

Step 13: Periodic Internal Audit

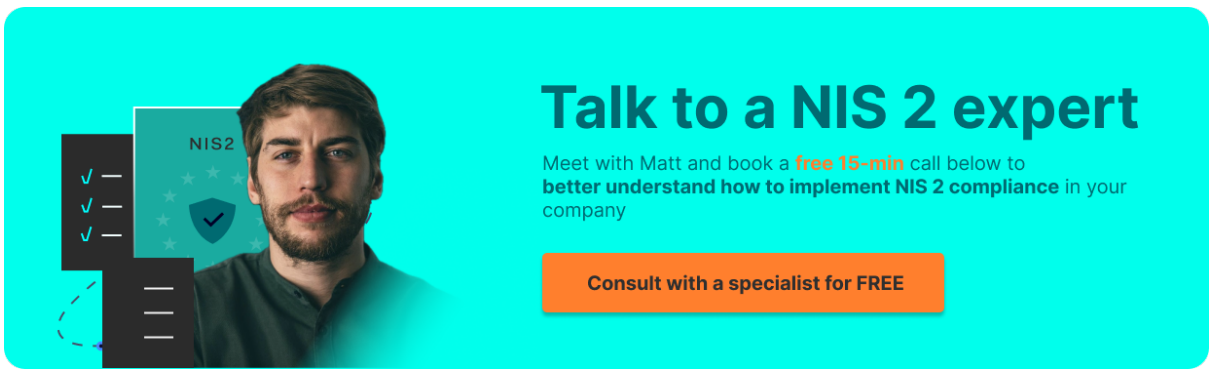
While not mentioned in NIS2, internal audits are recommended by ISO 27001 and other standards. They help senior management oversee cybersecurity implementation by identifying nonconformities.

Step 14: Periodic Management Review

Hold formal management review meetings to provide senior management with relevant cybersecurity information (e.g., Measurement Report, Internal Audit Report). These reviews enable key decisions on cybersecurity.

Step 15: Execute Corrective Actions

Implement a systematic approach to resolve nonconformities. Analyze the cause of each issue and define activities to eliminate it, ensuring similar nonconformities do not recur.



List of required documents and policies

The table below outlines the NIS2 requirements, relevant articles from Chapter IV of the Directive, and best practices for documenting these requirements.

What must be documented	NIS 2 article	Usually documented through
Management bodies must approve the cybersecurity risk-management measures	Article 20, paragraph 1	Risk Treatment Plan
Management bodies must oversee the implementation of cybersecurity risk-management measures	Article 20, paragraph 1	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	Training and Awareness Plan
Entities must take appropriate and proportionate technical, operational, and organizational measures to manage the risks	Article 21, paragraph 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	Risk Assessment Methodology + Risk Assessment Table
Policy on risk analysis	Article 21, paragraph 2, point (a)	Risk Assessment Methodology
Policy on information system security	Article 21, paragraph 2, point (a)	Policy on Information System Security
Incident handling	Article 21, paragraph 2, point (b)	Incident Management Procedure + Incident Log
Business continuity	Article 21, paragraph 2, point (c)	Business Continuity Plan
Backup management	Article 21, paragraph 2, point (c)	Backup Policy
Disaster recovery	Article 21, paragraph 2, point (c)	Disaster Recovery Plan
Crisis management	Article 21, paragraph 2, point (c)	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)	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)	Secure Development Policy + Specification of Information System Requirements
Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	Article 21, paragraph 2, point (f)	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)	IT Security Policy

Cybersecurity training	Article 21, paragraph 2, point (g)	Training and Awareness Plan
Policies and procedures regarding the use of cryptography and encryption	Article 21, paragraph 2, point (h)	Policy on the Use of Encryption
Human resources security	Article 21, paragraph 2, point (i)	Security Policy for Human Resources
Access control policies	Article 21, paragraph 2, point (i)	Access Control Policy
Asset management	Article 21, paragraph 2, point (i)	Asset Management Procedure + Inventory of Assets
The use of multi-factor authentication or continuous authentication solutions	Article 21, paragraph 2, point (j)	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	Supplier Security Policy + Risk Assessment and Treatment Report
Take appropriate and proportionate corrective measures	Article 21, paragraph 4	Procedure for Corrective Action + Corrective Action Form
Notify CSIRT or competent authority of significant incident	Article 23, paragraph 1	Significant Incident Notification for CSIRT/Competent Authority
Notify the recipients of services of significant incidents that are likely to adversely affect the provision of those services	Article 23, paragraph 1	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	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)	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)	Significant Incident Notification for CSIRT/Competent Authority
An intermediate report on relevant status updates	Article 23, paragraph 4, point (c)	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)	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)	Significant Incident Progress Report

Common cybersecurity documents that are not required by NIS 2

Besides the required documents listed above, it is also recommended to have the following documents in place:

- **Information Classification Policy** — provides clear rules on how to classify documents and other information, and how to protect those assets according to classification level.
- **Mobile Device, Teleworking 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.
- **Procedures for Working in Secure Areas** — defines security rules for data centers, archives, and other areas that need special protection.
- **Change Management Policy** — defines rules on how to perform changes in production systems, in order to decrease security risks.
- **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.

How to report incidents

The NIS2 Directive specifies reporting obligations in Article 23, which is detailed and demanding. Here is a breakdown of which incidents need to be reported, to whom, and how to do so.

What is a Significant Incident According to NIS2?
Under NIS2, an incident is defined as “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.”
Only significant incidents must be reported.

A significant incident is defined as one that has a substantial impact on the provision of services by essential and important entities 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 NIS2 mentions that indicators such as the extent of service disruption, incident duration, and the number of affected service recipients play a crucial role in identifying whether the operational disruption is severe.
However, there are no specific guidelines on what constitutes "severe financial loss" or "considerable material or non-material damage."
Both essential and important entities must report significant incidents; there are no requirements to report other types of incidents.

To Whom Are Incidents Reported?

NIS2 requires essential and important entities to notify the following parties of significant incidents:

- The Computer Security Incident Response Team (CSIRT) or a competent authority designated by Member States to be responsible for cybersecurity and supervisory tasks.
- Recipients of services from essential or important entities that are potentially affected by the significant incident.

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 22, 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	Significant Incident. Notification for Recipients of Services
An early warning (for CSIRT or competent authority)	Article 22, paragraph 4, point (a)	Without undue delay and in any event, within 24 hours of becoming aware of the significant incident undue	Indicates whether the significant incident si suspected of being caused by unlawful ro 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, ni 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 wel 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	SignificantIncident 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; i) the type of threat or root cause that is likely ot have triggered the incident; ii) applied and ongoing mitigation measures; (in) where applicable, the cross-border impact of the incident	Significant Incident Final Report
Aprogress 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

Talk to a NIS 2 expert

Meet with Matt and book a free 15-min call below to **better understand how to implement NIS 2 compliance** in your company

Consult with a specialist for FREE

Performing training and awareness according to NIS 2

The NIS2 Directive mandates that all employees, including senior management, must undergo cybersecurity training. Here's a guide on where to start, which topics to cover, and how to organize the entire process.

Topics to Cover in NIS2 Cybersecurity Training and Awareness

Chapter IV of NIS2 outlines 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 topics will be appropriate for everyone in the company, so the topics are separated according to the target audience.

Topics for All Employees (including mid-level and senior management)

- Basics of the NIS2 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)
- Use of multi-factor authentication and continuous authentication solutions (Article 21, paragraph 2, point j)

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 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)

Topics for Professionals Close to Security Management

- Steps for NIS2 compliance (relevant articles in Chapter IV)
- Relationship between NIS2 and ISO 27001 (Preamble recital 79, Article 21, paragraph 1, Article 25)
- Relationship between NIS2 and DORA (Preamble recital 28)
- Relationship between NIS2 and CER (Article 2, paragraph 3, Article 3, paragraph 1, point 5)
- Relationship between NIS2 and GDPR (Preamble recital 121, Article 35)
- Certification of IT products and services (Article 24)
- Government bodies defined in NIS2 (various articles)
- Organizing regular cybersecurity trainings for different employee levels (Article 20, paragraph 2; Article 21, paragraph 2, point g)
- Performing risk assessment and treatment according to NIS2 (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)

Topics for Top Management and Security Managers

- Identification of essential and important entities that must comply with NIS2 (Article 4)
- Main cybersecurity requirements of NIS2 (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)
- NIS2 fines and liabilities (Article 20, paragraph 1; Article 32, paragraph 6; Article 34)
- Cybersecurity legislation by EU countries (Article 41)

The Process of Setting Up NIS2 Training

To set up cybersecurity training compliant with NIS2, follow these steps:

1. **Assess the risks in the company:** This is the basis for writing security documents and identifying training focus areas.
2. **Define cybersecurity policies and procedures:** Clarifies roles and responsibilities.
3. **Define target groups for training:** Different groups based on their cybersecurity roles.

4. **Define training topics:** Tailored to risks, roles, and responsibilities of various target groups.
5. **Determine training frequency, measurement, and responsibility:** Establish how often training will occur, how it will be evaluated, and who will oversee it.

Options for Delivering Training Regularly

Several options are available for delivering NIS2 cybersecurity training:

Instructor-led In-Classroom Training

- **Pros:**
  - Adaptable to company needs
  - Higher engagement
- **Cons:**
  - Expensive
  - Infrequent
  - Challenging to separate training for different target groups

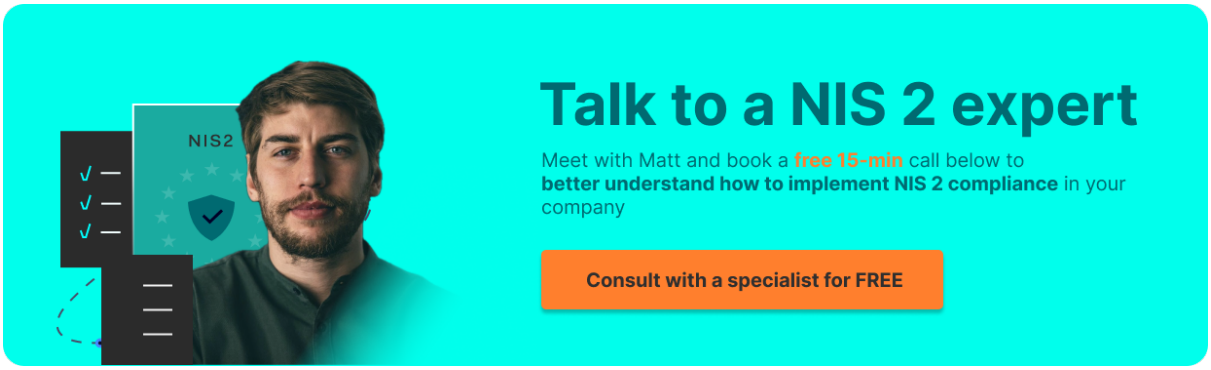
Instructor-led Online Training

- **Pros:**
  - Adaptable to company needs
- **Cons:**
  - Lower engagement

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
  - Cost-effective
- **Cons:**
  - No direct interaction with the instructor

By following these steps and utilizing the appropriate training methods, companies can ensure comprehensive and effective cybersecurity training in line with NIS2 requirements.



NIS 2 synergies with other frameworks and regulations

How is NIS2 Related to ISO 27001?
While NIS2 does not mandate the implementation of ISO 27001, **it references the ISO/IEC 27000 series** in its preamble as a means to implement cybersecurity risk management measures.

The main body of NIS2 encourages the use of international standards.
A closer comparison of NIS2 and ISO 27001 reveals that ISO 27001 provides an excellent framework for meeting the cybersecurity risk management measures required by NIS2. ISO 27001 offers clear guidelines on defining the risk management process, integrating technical implementations with training and HR issues, and involving top management.

What is the Difference Between NIS2 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).”

Although both NIS2 and GDPR focus on data protection, they differ significantly:

1. **Scope and Focus:**
    - **NIS2:** Primarily targets the security of network and information systems of essential and important entities to ensure the continuity of essential services.
    - **GDPR:** Concentrates on protecting the personal data of individuals and their privacy rights.
2. **Objectives:**
    - **NIS2:** Aims to improve the overall level of cybersecurity across the EU.
    - **GDPR:** Seeks to harmonize data protection laws across the EU and protect individuals’ privacy.
3. **Compliance Requirements:**
    - **NIS2:** Focuses on implementing cybersecurity measures, risk management, and incident reporting.
    - **GDPR:** Emphasizes lawful data processing, data subject rights, and data breach notifications.
4. **Enforcement and Penalties:**
    - **NIS2:** Enforcement involves national authorities designated for cybersecurity; penalties vary by member state.

- **GDPR:** Enforcement is carried out by data protection authorities with significant penalties for non-compliance, up to 4% of global annual turnover or €20 million, whichever is higher.

Understanding these differences is crucial for organizations that must comply with both NIS2 and GDPR, ensuring they address the unique requirements of each framework effectively.

	NIS 2	EU GDPR
Type	Directive (companies comply with local legislation that is published)	Regulation (directly applicable ot companies)
Applies to	Organizations that are considered essential and important entities	Any organization that processes personal data
Protection	Cybersecurity measures are applied ot al data within the company	Cybersecurity measures apply to personal data only; there si also a legal aspect of protection of personal data

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).

There will be audits performed from 2026 onward, which will happen “unexpectedly” and validate the controls and measures implemented within company against the NIS 2 regulative. In case there will be gaps, sanctions will be applied to the respected company.

NIS 2
Compliant.org

NIS 2 Compliant.org

About us.

Curated by NIS2Compliant.org, this page provides publicly-sourced information on everything related to the upcoming NIS2 Directive. Presented in a clear and concise manner for easy consumption.

More info:

Contact: become@nis2compliant.org
Web: www.nis2compliant.org
Ask us anything: www.nis2compliant.org/get-all-the-answers-you-need/
Book FREE Consultation: https://calendly.com/benchmarked_/call

Disclaimer

The information provided on this website is intended for educational and informational purposes only. The content is not intended to be a substitute for professional advice or any other legal advisory, service, etc. Theis guide's administrators and contributors make no representations or warranties of the information on the site. Any reliance you place on such information is therefore strictly at your own risk. The information is gathered from public information on internet and official literature of NIS 2 directive.