HOLM SECURITY

NIS2
Reference Guide

NIS2 seeks to further enhance the work started in the NIS Directive to create a more resilient and secure cyber security environment within the European Union.

www.holmsecurity.com/nis2

Table of Contents

1 NIS2 Introduction

The NIS2 Directive will take effect in October 2024 and seeks to enhance the work further started with the NIS Directive.

1

NIS2 Introduction

Taking effect in October 2024, the NIS2 Directive aims to establish a higher level of cyber security and resilience within organizations of the European Union. NIS2 largely follows the same principles as NIS but with several important additions, bringing more sectors into scope and providing guidelines to ensure uniform ratification into local law across EU member states.

New in NIS2

- ✓ More entities and sectors (industries) covered
- ✓ Greater accountability for management and personal responsibility
- ✓ New methods of selection and registration
- ✓ New incident notification deadlines
- ✓ Applies “directly” to essential/important entities and “indirectly” to suppliers
- ✓ Mandatory incident reports, also for so-called “near-misses”
- ✓ Introduction of sanctions, like those included in GDPR

Three Main Pillars of NIS2

MEMBER STATE RESPONSIBILITIES

- National Authorities
- National Strategies
- CVD Frameworks
- Crisis Management Frameworks

COMPANY RESPONSIBILITIES

RISK MANAGEMENT

- Accountability for top management for non-compliance
- Essential and important companies are required to take security measures
- Companies are required to notify incidents within a given time frame

COOPERATION AND INFO EXCHANGE

- Cooperation group
- CSIRTs Network
- CyCLONe
- CVD and European Vulnerability registry
- Peer-reviews
- Biennial ENISA cyber security report

2 NIS2 Extension of Scope

NIS2 increases the number of sectors involved and redefines organizations in scope as “Essential” and “Important” entities.

2

Essential & Important Entities

The former distinction between Operators of Essential Services (OES) and Digital Service Providers (DSPs) in the original NIS Directive is replaced by a distinction between Essential Entities (EE) and Important Entities (IE). The distinction between the two depends on factors such as size, sector, and criticality to society. Both entity types must follow the NIS2 framework for cyber security, but essential entities have stricter reporting and supervision requirements.

Essential entities

These entities are subject to immediate supervision (proactive).

Important entities

These entities are subject to ex-post supervision (reactive).

Large entity

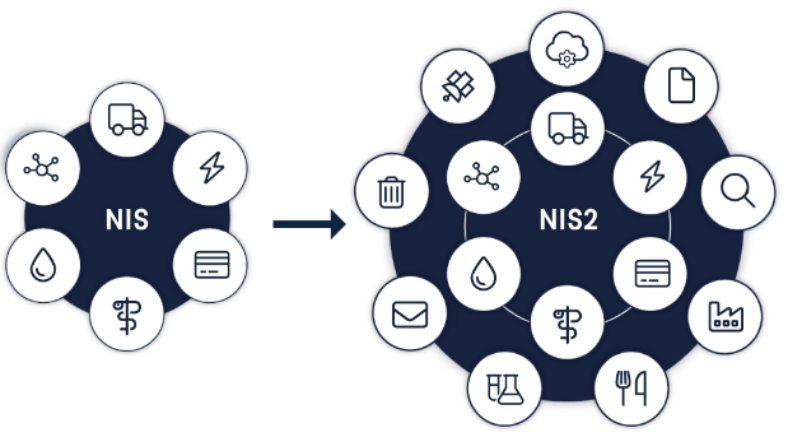
The NCSC defines large entities as those with a headcount of over 250 or more than €50 million in revenue.

Medium entity

The NCSC defines medium entities as those with a headcount of over 50 or more than €10 million in revenue.

The National Cyber Security Centre (NCSC) has defined a list of sectors that fall under the NIS2 umbrella and established a base rule that any large or medium entity from those sectors will be directly included in the scope. This does not necessarily exclude small or micro-organizations; member states can extend these requirements if an entity fulfills specific criteria as a key player in society, the economy, particular sectors or types of service.

The first version of NIS impacted a limited number of sectors but with NIS2 comes extended coverage to a total of 15 industries.



Essential & Important Entities

Sector	Sub-Sector	Large Entities (>250 staff or >€50 million revenue)	Medium Entities (50-249 staff or >€10 million revenue)	Small/Micro Entities (S: <50 staff or <€10 mil. revenue; M: <10 staff or <€2 mil. revenue)
Sectors of high criticality				
Energy	Including subsectors electricity, oil, and gas.	Essential	Important	Not in Scope
Transportation	Including subsectors of air transport, rail transport, shipping, and road transport.	Essential	Important	Not in Scope
Health	Including subsector healthcare environments (including hospitals and private clinics).	Essential	Important	Not in Scope
Public Administration	Of central governments.*	Essential	Essential	Essential
	Of regional governments.	Important	Important	Important
Banking & Financial Market Infrastructure	Banks and financial market infrastructure, e.g. payment services.	Essential	Important	Not in Scope
Digital Infrastructure	Qualified trust service providers, DNS service providers, and TLD name registries.	Essential	Essential	Essential
	Providers of public electronic communications networks.	Essential	Essential	Important
	Non-qualified trust service providers.	Essential	Important	Important
	Internet exchange point, cloud computing service, data center service, and content delivery network providers.	Essential	Important	Not in Scope
Water Supply	Including drinking water and wastewater, the latter of which **only** applies if it is an essential part of the entities' general activity.	Essential	Important	Not in Scope
Space	Operators of ground-based infrastructure.	Essential	Important	Not in Scope

* Excluding judiciary, parliaments, central banks, defense, national or public security.

Essential & Important Entities

Other critical sectors

Sector	Sub-Sector	Large Entities (>250 staff or >€50 million revenue)	Medium Entities (50-249 staff or >€10 million revenue)	Small/Micro Entities (S: <50 staff or <€10 mil. revenue; M: <10 staff or <€2 mil. revenue)
Postal & Courier Services		**Important**	**Important**	**Not in Scope**
Waste Management	(*Only* if principal economic activity).	**Important**	**Important**	**Not in Scope**
Chemicals	Manufacture, production, and distribution.	**Important**	**Important**	**Not in Scope**
Food	Wholesale production and industrial production and processing.	**Important**	**Important**	**Not in Scope**
Manufacturing	(In vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment.	**Important**	**Important**	**Not in Scope**
Digital Providers	Online marketplaces, search engines, and social networking platforms.	**Important**	**Important**	**Not in Scope**
Research	Research organizations (excluding education institutions).	**Important**	**Important**	**Not in Scope**
Entities Providing Domain Name Registration Services	All sizes, but only subject to Article 3(3) and Article 28			

There are certain exceptions to the above guide. Please consult the text of the Directive for a full and comprehensive list of all exceptions.

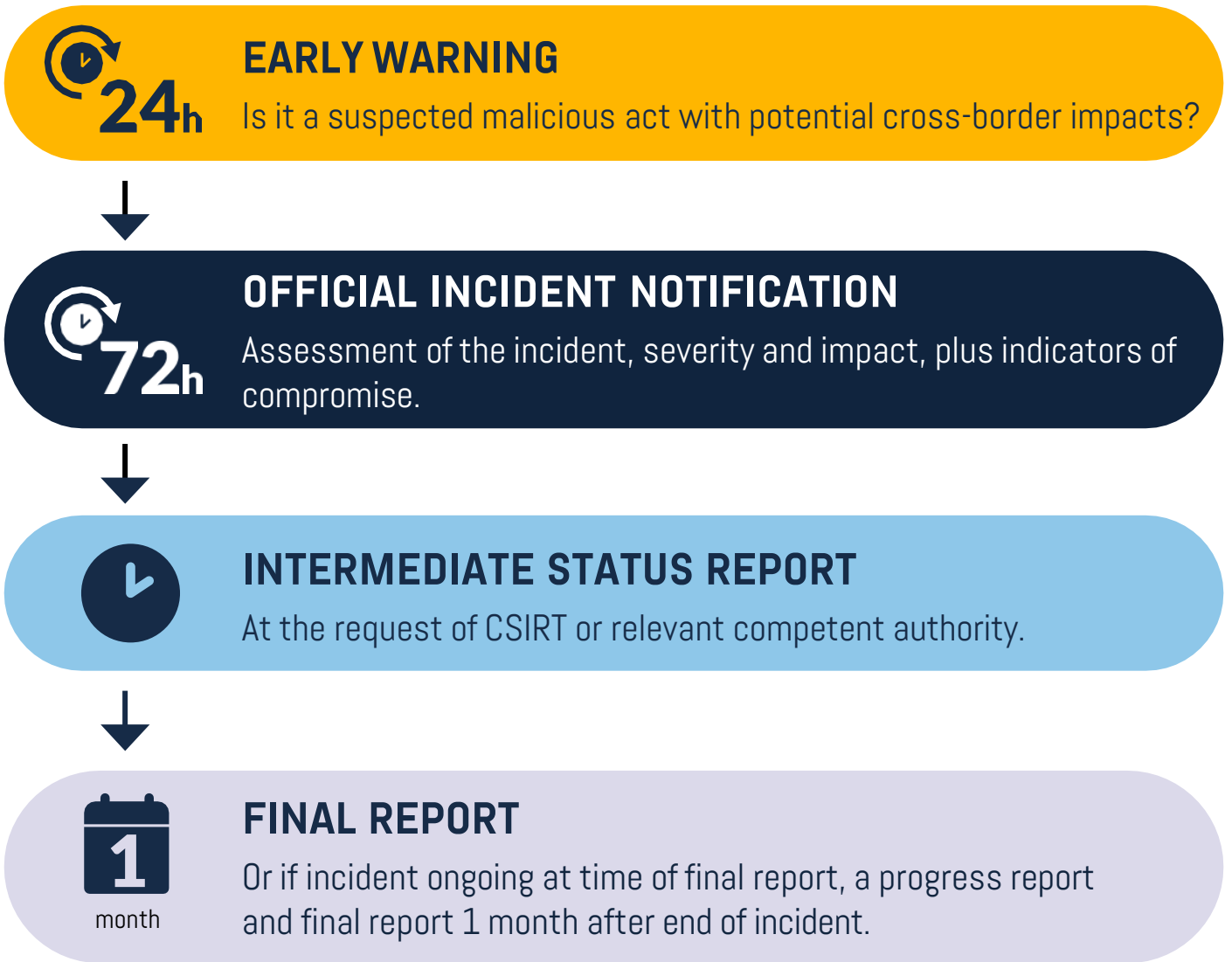
3 NIS2 Incident Reporting

As already established for NIS, every member state will have a central point of contact for compliance with the Directive.

3 Incident Reporting

As already established for NIS, every member state will have a central point of contact for compliance with the Directive as well as a coordinating Computer Security Incident Response Team (CSIRT) or other competent authority for incident reporting. In Belgium, for example, this will be the role of the Centre for Cyber Security Belgium (CCB).

The CSIRT or competent authority must report such incidents to ENISA every three months using anonymized information. With this data, ENISA will then report on EU incidents every six months. This reporting process will help organizations and EU member states to learn from such incidents and is a crucial change in the new NIS2 Directive.



Where appropriate, entities shall notify the recipients of their services of significant incidents.

When in the public interest, the CSIRT or relevant competent authority may inform the public about the significant incident or may require the entity to do so.

HOLM SECURITY

4 NIS2 Stricter Penalties & Jurisdictional Complexities

NIS2 introduces stricter penalties for non-compliance than those found in NIS and emphasizes cross-border compliance and cooperation.

4

Stricter Penalties for Non-Compliance

NIS2 introduces stricter penalties for non-compliance by essential and important entities, including fines of up to 2% of an entity's annual turnover.

Essential Entities

Administrative fines of up to €10,000,000 or 2% of the total annual worldwide turnover in the previous fiscal year, whichever amount is higher.

Important Entities

Administrative fines of up to €7,000,000 or 1.4% of the total annual worldwide turnover in the previous fiscal year, whichever amount is higher.

Jurisdictional Complexities

Under the NIS2 Directive, essential and important entities fall under the jurisdiction of the EU member state where they provide their services. If the entity provides services in more than one member state, each of these member states has jurisdiction. For entities where the service is provided or is dependent on operations outside the EU, they must ensure that they can continue operating within the EU should their non-EU operations stop.

HOLM SECURITY

5 NIS2 Management Responsibilities

NIS2 obligates senior management to take ownership of their organizations' cyber security maturity level. Failure to do so bears serious consequences.

5

Management Responsibilities

Management accountability is yet another cornerstone of NIS2, as the new Directive will obligate management to take ownership of their organizations' cyber security maturity level. This will include conducting risk assessments and approving risk treatment plans, meaning management must partake in cyber security training. The Directive also mandates organizations train their employees on cyber security risk and response.

Failure by management to comply with NIS2 requirements could result in serious consequences, including liability, temporary bans, and administrative fines as provided for in the implementing national legislation.

Management bodies of essential and important entities must:

- **Approve the adequacy** of cyber security risk management measures taken by the entity
- **Supervise the implementation** of risk management measures
- **Follow training** to gain sufficient knowledge and skills to identify risks and assess cyber security risk management practices and their impact on the services provided by the entity
- **Offer similar training to their employees** on a regular basis
- **Be accountable** for non-compliance

HOLM SECURITY

6 NIS2 Risk Management Measures

Essential and important entities must take appropriate and proportional technical, operational and organizational measures to manage risks.

6

Risk Management Measures

Risk management is a crucial component of NIS and NIS2 compliance, providing a systematic and structured approach to identifying, analyzing, and managing risks associated with IT infrastructure. The European Union Agency for Cybersecurity (ENISA) specifically mentions risk (vulnerability) management as one of the ways to improve cyber security in the EU member states.

Article 21 of the NIS2 Directive summarizes the minimum measures entities under NIS2 must take. These measures clearly state the need for risk analysis and risk management.

Article 21 (2a)

Policies on risk analysis and information system security.

Article 21 (2a)

Policies and procedures to assess the effectiveness of cyber security risk-management measures.

Such measures must include at least the following:

1. Risk analysis & information system security
2. Incident handling
3. Business continuity measures (back-ups, disaster recovery, crisis management)
4. Supply chain security
5. Security in system acquisition, development and maintenance
6. Policies and procedures to assess the effectiveness of cyber security risk management measures
7. Basic computer hygiene and training
8. Policies on the appropriate use of cryptography and encryption
9. Human resources security, access control policies, and asset management
10. Use of multi-factor, secured voice/video/text comm & secured emergency communication

HOLM SECURITY

7

NIS2

Automated & Continuous Risk Assessments

Risk management is a crucial component of NIS2 compliance and Article 21 of the NIS2 Directive clearly states the need for risk analysis.

7

Automated & Continuous Risk Assessments

Risk assessments are essential in the context of NIS and NIS2, as they play a fundamental role in identifying, evaluating, and managing cyber security risks within critical infrastructure and essential services. The NIS directives emphasize the importance of risk assessments as part of a broader strategy to enhance the overall cyber security resilience of organizations covered by the directives.

Performing continuous risk assessments as part of the vulnerability management workflow creates a systematic approach toward cyber threats. This approach positions your organization as proactive, meaning you will focus on preventing incidents rather than cleaning up after the fact.

Risk assessments are essential and help your organization:

HOLM SECURITY

8 NIS2 Cyber Hygiene Requirements

Over 90% of all incidents start with a human element so the EU has included cyber hygiene practices and cyber security training as part of NIS2.

8

Cyber Hygiene Requirements

Research shows that over 90% of all incidents start with a human element. As a response, the EU has included cyber hygiene practices and cyber security training as part of the NIS2 Directive. This can be found in Article 21, section 2G ("basic cyber hygiene practices and cyber security training").

Cyber hygiene refers to the measures individuals and organizations must take to maintain good cyber security health and protect their digital environments from cyber threats. It involves taking proactive and preventive steps to reduce the risk of cyberattacks and ensure the overall security of information systems.

Key aspects of cyber hygiene:

- **Password management**
- **Software updates and patching**
- **Phishing awareness and training**
- **Data backups**
- **Mobile device security**
- **Secure Wi-Fi best practices**
- **Incident response planning**
- **Secure web browsing**
- **IoT security**
- **Firewall and security software**
- **Access control**
- **Compliance with regulations**

HOLM SECURITY

9

NIS2

Holm Security Takes You There

We provide complete packages to fully support your risk-based efforts to comply with NIS2 – all in one platform.

9

Holm Security Takes You There

Holm Security has helped hundreds of organizations throughout the EU comply with the NIS Directive and is now helping hundreds more comply with NIS2. We provide the tools you need to take impactful steps toward compliance.

These tools allow you to:

- Perform automated and continuous (systematic) risk assessments
- Create a proactive approach towards cyber security
- Implement basic cyber hygiene practices and cyber security training
- Provide the tools needed to secure the supply chain
- Help management supervise the implementation of risk management
- Demonstrate compliance based on data and reports

NIS2 Requirement	Our Solution
Take systematic, analytical, risk-based steps within information security and perform risk assessments.	We provide a market-leading platform for automated and continuous risk assessments (vulnerability management).
Implement basic cyber hygiene practices and cyber security training.	We help customers strengthen their human defense against phishing attacks with phishing simulation and tailored and automated awareness training.
Essential and important entities, as well as their suppliers, must conduct risk assessments.	We do risk assessments for customers and their suppliers both in the initial phase as well as daily maintenance.
Demonstrate compliance today and in the future.	Our reports and data show compliance from the very first day of usage.
Management supervises the implementation of risk management.	Our platform can fully automate the process for management to supervise continuous risk assessments based on easy-to-consume statistics and data.
Administrative sanctions, lost permits, certifications, and penalties.	We help prevent these scenarios by proactively finding and mitigating risks or vulnerabilities.

HOLM SECURITY

10 NIS2 Frequently Asked Questions

Understanding NIS and NIS2 is a challenge for most organizations. We are here to help you understand and meet the new requirements.

10 Frequently Asked Questions

What is the key purpose of NIS2?

Increasing Cyber Security Resilience

NIS2 encourages EU member states and critical infrastructure operators to enhance their cyber security resilience and preparedness to respond to, and recover from, cyber incidents effectively.

Harmonizing Cyber Security Standards

It seeks to harmonize cyber security standards and practices across the EU to ensure a consistent and high level of security across the digital landscape.

Mandatory Reporting of Incidents

NIS2 mandates the reporting of significant cyber incidents to national authorities and establishes a coordinated mechanism for sharing information on cyber threats and incidents among member states.

Critical Infrastructure Protection

The Directive places a special focus on protecting critical infrastructure sectors, such as energy, transportation, healthcare, and digital infrastructure by requiring them to meet specific cyber security requirements.

Enforcement and Penalties

NIS2 introduces measures for effective enforcement of cyber security requirements and penalties for non-compliance, thereby incentivizing organizations to invest in cyber security measures.

Cooperation and Information-sharing

It promotes cooperation and information sharing among member states and between the public and private sectors to enhance collective cyber security defense.

When will NIS2 come into effect?

The NIS2 Directive is set to be ratified by all EU member states by 17 October 2024. This is a crucial date for businesses to take note of, as failure to comply with the Directive can result in severe consequences such as financial penalties and damage to reputation. That said, it's essential that companies gear up and make necessary preparations to ensure full compliance well before the deadline. Don't wait until it's too late - act now to avoid any potential negative consequences.

10 Frequently Asked Questions

How do I know if my organization must comply with NIS2?

The steps to NIS2 compliance may vary based on specific national implementations or industry requirements, but the first step is to determine whether your organization falls under the scope of NIS2. Identify whether you are an essential or important entity according to the definitions provided in the Directive, then follow the remaining **10 steps to compliance**.

What are the NIS2 fines?

The NIS2 Directive takes a nuanced approach to administrative fines, differentiating between the two types of entities.

Essential entities
Administrative fines of up to €10,000,000 or 2% of the total annual worldwide turnover in the previous fiscal year, whichever amount is higher.

Important entities
Administrative fines of up to €7,000,000 or 1.4% of the total annual worldwide turnover in the previous fiscal year, whichever amount is higher.

When complying with NIS/NIS2, what must we consider regarding our suppliers?

One of the focus areas of NIS2 is securing the supply chain. This means that both your organization **and your suppliers** must meet the criteria of NIS2 compliance. It is your responsibility to make sure that your suppliers do so.

I'm a supplier to an organization that must comply with NIS/NIS2 – what should I consider?

As a supplier to an organization that must comply with NIS/NIS2, you must ensure that you meet NIS/NIS2 security requirements.

10 Frequently Asked Questions

What is the difference between essential & important entities?

The difference between them lies not in which requirements they must meet, as these remain the same for both entities, but rather in which supervisory measures and penalties will apply. Entities in both categories will have to meet the same requirements. However, the distinction will be in the supervisory measures and penalties. Essential entities will be required to meet supervisory requirements as of the introduction of NIS2, while the important entities will be subject to ex-post supervision, meaning that action is only taken if and when in case authorities receive evidence of non-compliance.

Is vulnerability management required for compliance with NIS2?

Regarding the requirements put down by the EU and local authorities, vulnerability scanning, or security scanning, is a requirement as part of risk assessment. The National Cyber Security Centre (NCSC) of Ireland and The Swedish Civil Contingencies Agency (MSB) refer to vulnerability management as a key element in compliance with the NIS2 Directive.

What is the difference between NIS/NIS2 and DORA?

The Digital Operational Resilience Act, or DORA, is a European Union (EU) regulation that creates a binding, comprehensive information and communication technology (ICT) risk management framework for the EU financial sector. DORA has many similarities with NIS and NIS2, like the risk-based approach, but is limited to the financial sector, while NIS2 applies to many industries indispensable to society.

10 Frequently Asked Questions

How can Holm Security help my organization comply with NIS2?

Implementing risk-based cyber security practices is one of the most important areas of NIS and NIS2. Holm Security helps organizations that must comply with NIS and NIS2:

- ✓ Perform automated and continuous (systematic) risk assessments.
- ✓ Create a proactive approach towards cyber security.
- ✓ Implement basic cyber hygiene practices and security training.
- ✓ Provide the tools needed to secure the supply chain.
- ✓ Help management supervise the implementation of risk measures.
- ✓ Demonstrate compliance based on data and reports.

Contact Us

sales@holmsecurity.com

+46 8-550 05 582

Holm Security

Request a consultation