



Get your business ready for NIS2 directive before the deadline in 2024

In this whitepaper, you will learn the background, changes and objectives of NIS2 and what to expect in terms of oversight. You'll be able to see how your current cybersecurity program maps to the NIS2 requirements and learn how you can close the gaps and how Cybertrust can help to achieve this.

The NIS2 Directive



The latest version of the Network and Information Systems Directive (NIS2), which has been adopted by the EU member states, imposes stricter enforcement of cybersecurity requirements throughout the union and ensures uniform sanctions.

The directive will come into effect in 2024, which means that it will be mandatory for applicable organizations in the member states to comply with the new requirement.



Table of contents



- 01** What is the NIS2 Cybersecurity Directive?
- 02** Which sectors does NIS2 cover?
- 03** Does your organization fall within the new scope?
- 04** What requirements are placed on your organization?
- 05** Minimum measures you need to implement
- 06** What are the implications if you don't comply?
- 07** Cybertrust can help you to comply with NIS2



01 What is the NIS2 Cybersecurity Directive?

An increasingly digitized world and interconnectivity bring enormous opportunities for cyber-related threats.

NIS became the first EU-wide legislation on cybersecurity and the policy was adopted in 2016 to implement risk management and incident reporting obligations for specific entities. Also because of NIS, today there is a better understanding of the state of cybersecurity across Europe.

Over the years, the complexity and scale of cybersecurity incidents are growing, not only in terms of vectors and numbers but also in terms of their economic and social impact.

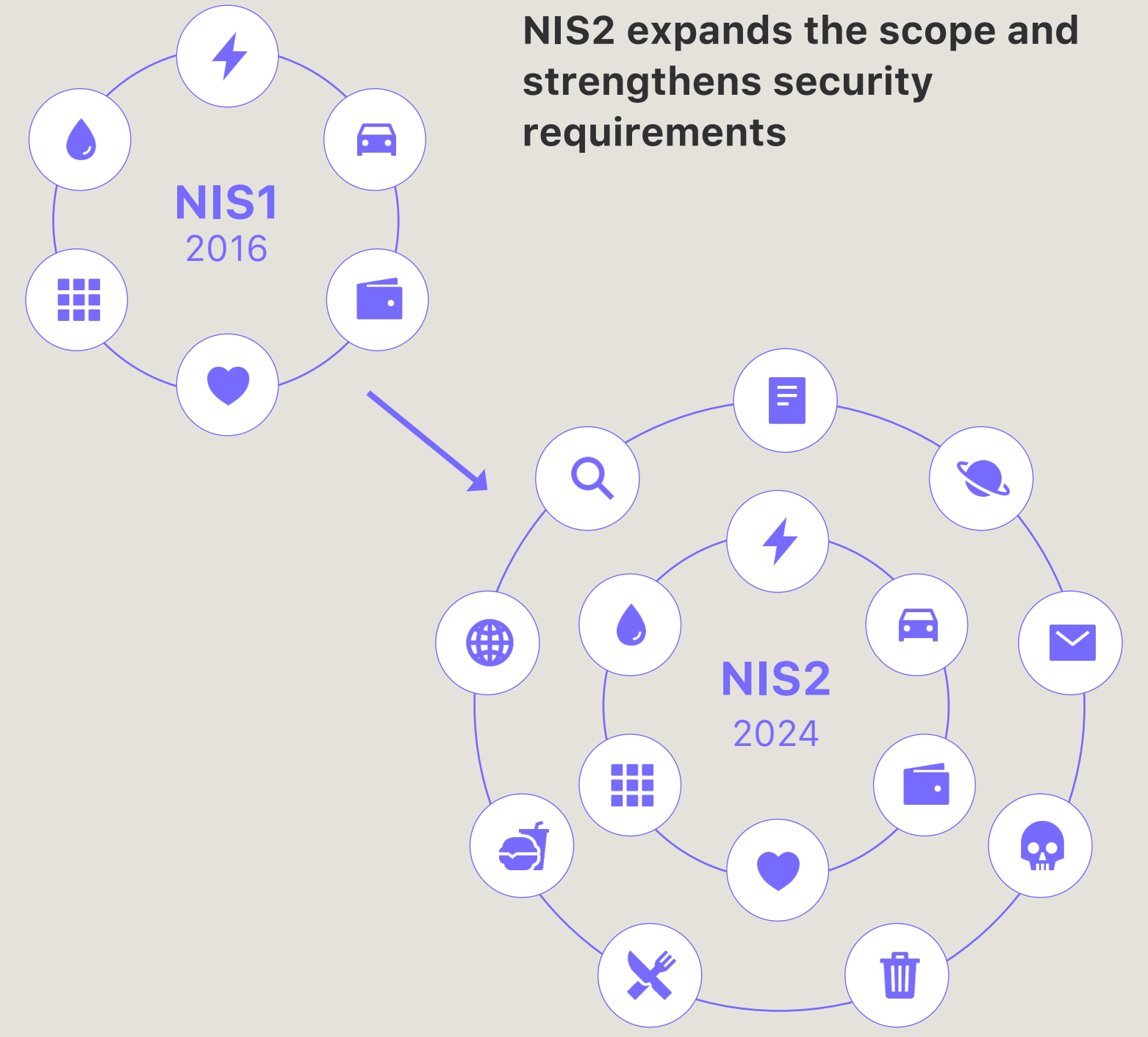
Due to these circumstances, the European Union recently adopted the revised version of the Network and Information Security Directive (NIS2), which provides legal measures to improve the overall level of cybersecurity in the EU, and among others, the EU-wide cooperation on incidents and threats.

The directive will manifest as national law, which means that each organization encompassed by the directive will be required to live up to its requirements.

What is new in the NIS2 Cybersecurity Directive?

NIS2 expands its EU-wide cybersecurity requirements and sanctions to harmonize and streamline the security level across all EU member states. The directive will manifest as national law, which means that each organization encompassed by the directive will be required to live up to its requirements and now must lay out clear plans for how they perform risk management, control and oversight.

NIS2 expands the scope and strengthens security requirements. The number of covered sectors is increasing because the NIS2 Commission wants all organizations who maintain a critical position in society to be encompassed by the directive in order to strengthen Europe's cyber resilience. This means that NIS2 will now also cover sectors such as food production, waste management digital providers and the entire supply chain.






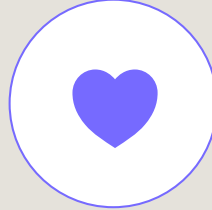











The NIS2 Directive is an extension of the original NIS Directive from 2016, which aimed to increase cybersecurity levels across the EU. NIS2 increases these cybersecurity requirements, enforcement of the requirements, and the level of fines for non-compliance.

02 Which sectors does NIS2 cover?



As a result, the NIS2 directive affects a lot more sectors than the original NIS directive. In the original version of NIS, entities were classified as Operators of Essential Services (OES) and Digital Service Providers (DSPs). NIS2 changes that with the introduction of classifying entities as either "essential" or "important," reflecting the extent to which their services are critical and their size.

When designing cybersecurity measures, member states should account for risk exposure of important and essential entities in terms of social and economic impact a successful cyberattack would have.








The following sectors are covered by NIS2:				
 Energy	 Transport	 Banking & Financial Market Infrastructure	 Health	 Drinking & Waste Water
 Digital Infrastructure	 Public Administration	 Space	 Postal Service	 Waste Management
 Chemicals	 Foods	 Production	 Digital Providers	 Research

03 Does your organization fall within the new scope?

Essential companies:

-  **Energy** – supply, distribution, transmission and sales
-  **Transport** – aerial, rail, road and sea
-  **Finance** – credit, trade, market and infrastructure
-  **Health** – research, production, providers and manufacturers
-  **Drinking & waste water**
-  **Digital infrastructure** – DNS, trust services, data center services, cloud computing, communication services, managed service providers and managed security providers.
-  **Public administration**, municipalities and regions
-  **Space** – software and services

Important companies:

-  **Postal** and parcel service
-  **Waste management**
-  **Chemical products** – production and distribution
-  **Foods** – production and distribution
-  **Production** of pharmaceutical, electronic and optical equipment and machinery and vehicles
-  **Digital providers** of online marketplaces, search engines, social platforms
-  **Research**

Source: European Commission

NIS2 greatly expands which organizations are impacted by its requirements and is careful to distinguish between “essential companies” and “important companies”.

The checklist below serves as a guide to understanding if you’re in scope and what topics are regulated:

For the two main types of entities only medium and large enterprises are in scope.

Medium-sized organizations with fewer than 250 employees and an annual turnover not exceeding 50 million euros (or balance sheet total of up to EUR 43 million) operating in highly critical sectors are considered important along with others large and medium-sized organizations in critical sectors.

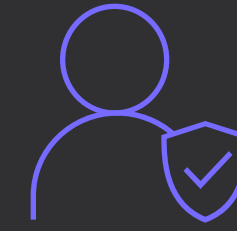
Large organizations exceeding the medium sized organizations and fall under highly critical sectors are considered “essential”.

You may still be impacted if:

- Your sector is in one of the above lists and your business is considered (by your Member State) as of national importance. This can be the case when the services provided are essential, the entity is the sole provider, and a service disruption has an impact on public safety, security or health.
- You have been identified as a critical entity. Critical entities are mandatorily also in scope of NIS2.
- You’re a services provider to a client that is considered in scope of NIS2.

04 What requirements are placed on your organization?

The NIS2 Directive adds new requirements for 4 primary areas of your organization: management, reporting to the authorities, risk management and business continuity. The purpose of this is to increase Europe's ability to withstand current and future cyberthreats.



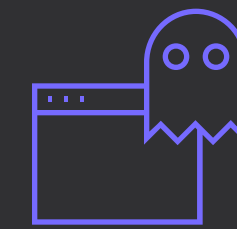
1. Management

It is necessary for management to be aware of and understand the requirements of the directive and the risk management efforts. They have a direct responsibility to identify and address cyber risks to comply with the requirements.



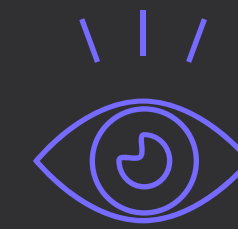
2. Reporting to the authorities

Organizations need to have established processes for ensuring proper reporting to authorities. There are requirements, for example, that major incidents should be reported within 24 hours.



3. Risk management

To meet the new requirements, organizations must implement measures to minimize risks and consequences. This includes incident management, improved supply chain security, network security, access control, and encryption.



4. Business continuity

Organizations must consider how to ensure business continuity in the event of major cyber incidents. This includes, for example, system recovery, emergency procedures, and establishment of a crisis response team.

05 Minimum measures you need to implement



It is not all the requirements of the directive that apply to all businesses and organizations.

Depending on the size of the business, the societal function and how exposed the organization is, the level of requirements varies. This is to ensure that the requirements remain proportionate, so that smaller businesses are not disproportionately affected, and that the requirements for larger businesses reflect their role in society. **That said, there are a number of minimum measures that NIS2 requires all relevant businesses to implement.**

As is the case with the 4 aforementioned focus areas, the following minimum measures (see next page) are general summaries of the directive's requirements areas and should not be considered fully comprehensive. To ensure that your specific business fully complies with the NIS2 directive, you should always seek advice from your compliance officer.



NIS2

minimum measures:

- 1 Risk assessments and security policies for information systems
- 2 A plan for handling security incidents
- 3 A plan for managing business operations during and after a security incident. This means that backups must be up to date. There must also be a plan for ensuring access to IT systems and their operating functions during and after a security incident.
- 4 Security around supply chains and the relationship between the company and direct supplier. Companies must choose security measures that fit the vulnerabilities of each direct supplier. And then companies must assess the overall security level for all suppliers.
- 5 Policies and procedures for evaluating the effectiveness of security measures.
- 6 Security around the procurement of systems and the development and operation of systems. This means having policies for handling and reporting vulnerabilities.
- 7 Cybersecurity training and a practice for basic computer hygiene.
- 8 Policies and procedures for the use of cryptography and, when relevant, encryption.
- 9 Security procedures for employees with access to sensitive or important data, including policies for data access. The company must also have an overview of all relevant assets and ensure that they are properly utilized and handled.
- 10 The use of multi-factor authentication, continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, when appropriate.

These descriptions are general summaries of the areas covered by the directive and are therefore not fully comprehensive. To ensure that your specific company complies with the NIS2 Directive, you should always seek advice from your compliance officer.

06 What are the implications if you don't comply?



Fines

Companies who don't comply with NIS2 once the directive has been put into effect in 2024, will be subject to significant fines based on whether they're categorized as essential or important companies.

Essential companies

Companies categorized as essential risk fines for up to €10 million euro or 2% of their global annual revenue.

Important companies

Companies categorized as important risk fines for up to €7 million euro or 1.4% of their global annual revenue.

Legal ramifications

The consequences of not being able to achieve NIS2 compliance now includes more than simply being eligible for fines. In addition, company management teams are now able to be held accountable for any failure to live up to the new requirements. In other words, the new directive now emphasizes management can face legal ramifications if they fail to adhere to the new rules.

Additionally, management need to take courses to improve their ability to assess cybersecurity risks and encourage their organization to offer similar courses for all employees on a regular basis.





Let **Cybertrust** help you comply with NIS2

No matter where you are in the cybersecurity journey from a basic understanding to more mature adoption, it's critical to significantly increase your level of resilience to secure the continuity of your organization and the eco system you are part of.

NIS2 comes with a substantial expansion of cybersecurity risk management and governance requirements and will require an effective approach which must be flexible enough to be adapted to different risk scenarios and organizational capabilities.

Cybertrust is a specialist in helping organizations comply with the NIS2 Directive and can provide expertise in developing incident response plans and risk assessments, as well as implementing technical and organizational security measures to ensure effective and sustainable security which can adapt along with the digital transformation of your organization now and towards the future.

cybertrust

SECURING THE WAY TO A SUSTAINABLE, RESILIENT FUTURE

Contact an expert about how Cybertrust can help you meet and secure the requirements of NIS2

I [cybertrust.eu](https://www.cybertrust.eu)

M contact@cybertrust.eu

Sustainable Cybersecurity

Cybersecurity sustainability means investing time, attention and capital in a way that mitigates risk, minimizes cost and maximizes effectiveness both now and in the long term.

With our consultancy services we can help to put these ideals into practice considering what sustainability looks like across the three pillars of security: people, process and technology.



Powered by **CRONOS**
GROEP