

NIS2 Directive: Achieve Compliance With Better Access Security

This guide gives you a short breakdown of the NIS2 directive from an access security perspective and offers concrete advice on how to live up to NIS2 requirements using a simple cybersecurity solution.



Made in Denmark

www.uniqkey.eu

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 requirements.

Table of Contents

-
- 01 **What is NIS2?**

 - 02 **Which sectors does NIS2 cover?**

 - 03 **Which organizations are impacted by NIS2?**

 - 04 **What requirements does NIS2 place on your organization?**

 - 05 **Minimum measures you need to implement**

 - 06 **How Uniqkey can help you comply with NIS2**

 - 07 **What happens if you don't comply with NIS2?**

 - 08 **Discover how Uniqkey protects critical infrastructure**

01 What is NIS2?

NIS2 stands for “**Network and Information Security Directive**” and is a continuation and expansion of the previous EU cybersecurity directive, NIS1. The aim of NIS2 is to strengthen the collective cybersecurity level of EU member states by increasing cybersecurity enforcement requirements for critical infrastructure sectors.

The NIS2 directive regulates companies and government agencies in the area of cybersecurity. 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.

NIS2 expands its EU-wide cybersecurity requirements and sanctions to harmonize and streamline the security level across all EU member states and stricter requirements means that your organization now has to lay

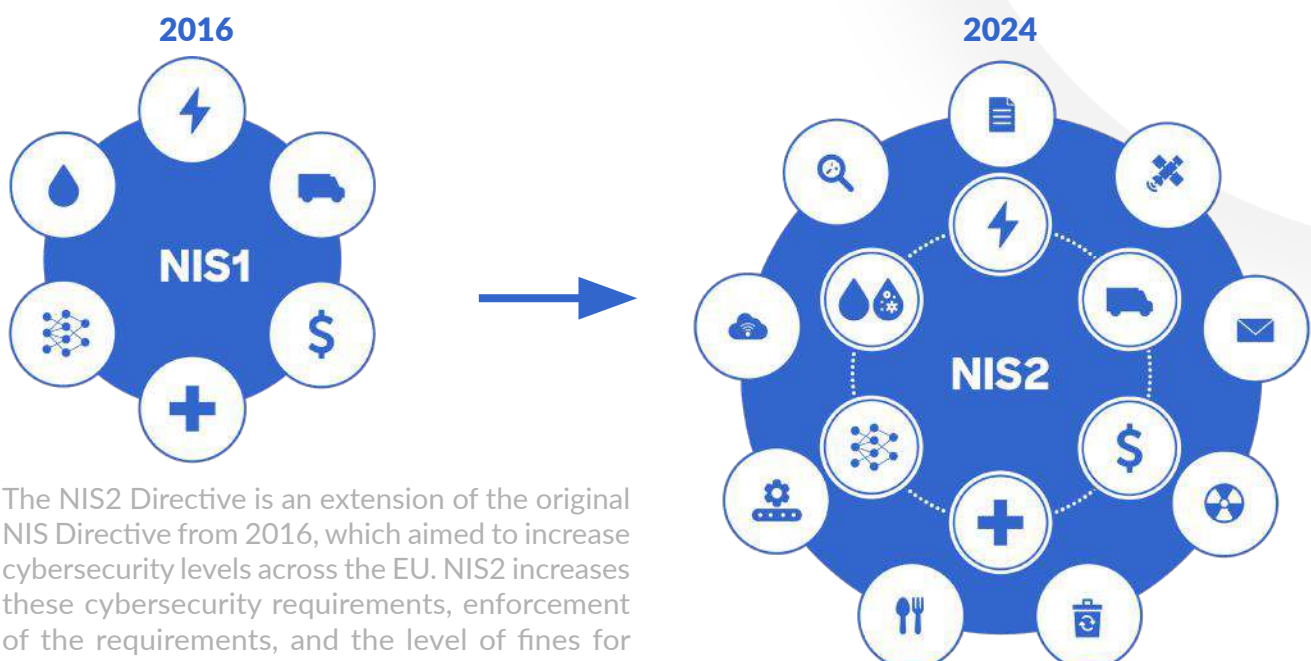
out clear plans for how they perform risk management, control and oversight.

What is the difference between GDPR and NIS2?

NIS2 is for European cybersecurity what GDPR was for European data protection.

Where GDPR strengthened the requirements for how EU member states manage personal data, the aim of NIS2 is to ensure that all European companies and organization that are considered a part of essential infrastructure maintain an adequate level of cybersecurity.

NIS2 expands the scope and strengthens security requirements



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?

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 and the entire supply chain.

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


Which organizations are impacted by NIS2?


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

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**

When does NIS2 go in effect?

The directive was passed by the European Parliament on November 10, 2022, and all applicable organizations and companies have until 2024 to comply with the new legal requirements after which they will be eligible for potential fines.

According to the directive, companies in the applicable sectors are obligated to understand and address the new rules, requirements and guidelines.

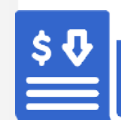
04 What requirements does NIS2 place on your organization?

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:

**The blue text marks which minimum measures Uniqkey can help cover.*

-
- 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

How Uniqkey can help you comply with NIS2

Based on the descriptions of the directive, it's possible to cover a range of the new NIS2 requirements and expectations by implementing Uniqkey.

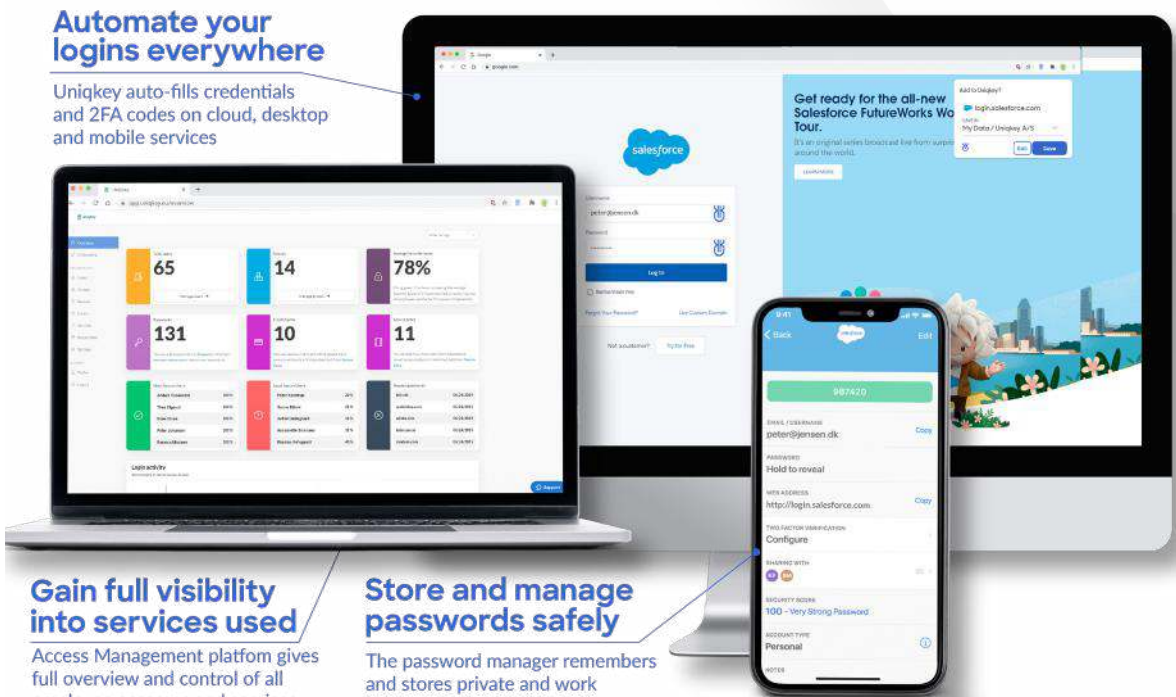
About Uniqkey

Uniqkey is Danish provider of a user-friendly business password & access management solution that helps businesses secure the use of passwords and streamline access management in a simple and easy way.



Automate your logins everywhere

Uniqkey auto-fills credentials and 2FA codes on cloud, desktop and mobile services



Gain full visibility into services used

Access Management platform gives full overview and control of all employee accesses and services

Store and manage passwords safely

The password manager remembers and stores private and work passwords safely

Uniqkey can help cover these minimum measures

Based on the descriptions of the directive, **it's possible to cover a range of the new NIS2 requirements and expectations by implementing Uniqkey.**

NIS2 Minimum measures

Pt 3:

Securing access to IT systems.

Uniqkey covers this by:

- ✓ **Managing, storing and saving all user logins securely.** And can be used without internet access.
- ✓ **Securing access to IT systems** and company services during operation with strong, unique passwords and two-factor authentication
- ✓ **Enabling admins to access a detailed audit log in** case of an incident

Pt 6:

Security around the procurement of systems and the development and operation of systems. This means having policies for handling and reporting vulnerabilities.

- ✓ **Offering data-driven security scores** for individual employees, service and work groups.
- ✓ Including a feature to **easily produce incident reports**

Pt 7:

Cybersecurity training and a practice for basic computer hygiene.

- ✓ **Increasing the user's security awareness** by informing about weak, reused or compromised passwords.
- ✓ **Facilitating a practice for basic computer hygiene** by supporting secure access to systems, replacing unsafe password storage habits, and minimizing incidents of unauthorized software use (Shadow IT)
- ✓ **Giving admins overview** of and insight into how secure each employee, service and work group really is.
- ✓ **Offering direct security training** via control panel with guides for 2FA setup and updating compromised passwords.

NIS2 Minimum measures

Pt 8:

Policies and procedures for the use of cryptography and, when relevant, encryption.

Pt 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.

Pt 10:

The use of multi-factor authentication, continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, when appropriate.

Uniqkey covers this by:

✓ **Encrypting the individual user's password** data offline and locally on their own device.

✓ **Securely storing** all company-relevant logins

✓ **Giving automatic overview of all IT assets**, employee accesses and supporting easy and secure employee onboarding and offboarding.

✓ **Supporting setup of extra security layers** and restrictions on business-critical systems and services.

✓ **Offering TOTP and continuous authentication** via biometric access security

✓ **Ensuring that all communication and data is encrypted** using TLS and public / private keys

07

What happens if you don't comply with NIS2?

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.

08 Discover how Uniqkey protects critical infrastructure

See how companies maintaining critical infrastructure use Uniqkey to increase their cyber resilience.

Danish Defence Testimonial



Curious about Uniqkey? Watch former CIO of the Danish Defence, Kristian Vengsgaard, talk about their comprehensive Uniqkey test.

Case Studies



[- Bornholms Energi - og Forsyning](#)
[- Vejle Brand Forsikring](#)

Uniqkey protects European critical infrastructure



Let Uniqkey help you comply with NIS2

Is NIS2 on your plate? Then let our product experts walk you through how Uniqkey covers essential NIS2 requirements, while facilitating instant measurable security for European companies who maintain critical infrastructure. Take action on NIS2 and contact us.

Contact our team on:

Email: nis2@uniqkey.eu

Phone: +45 71 96 99 67

