RESOURCE CENTER

How a password manager enables NIS2 compliance

Get the full interactive view at https://bitwarden.com/nl-nl/resources/how-a-password-manager-enables-nis2-compliance/

bitwarden

NIS2 is an expansion of the previous EU cybersecurity directive, NIS, which was adopted in 2016 as a set of requirements for securing network and information systems across the EU. NIS2 was introduced in 2020 and came into effect on January 16, 2023. As of October 17, 2024, all member states must meet its requirements.

The directive mandates businesses identified as operators of essential services to implement appropriate measures to enhance cybersecurity and comply with legal obligations. NIS2 encompasses several organizations that were not part of the original directive, expanding the affected sectors from 7 to 15 to protect even more vital areas. The list of entities included under NIS2 now includes:

- Energy
- Health
- Transportation
- Finance
- Water Supply
- Digital Infrastructure
- Public Administration
- Digital Providers
- Postal Services
- Waste Management
- Space
- Foods
- Manufacturing
- Chemicals
- Research

On top of that, NIS2 increases the requirements for enforcing cybersecurity, includes stricter rules for incident reporting, and has more severe penalties for noncompliance. Relevant authorities play a crucial role in supervising compliance and facilitating incident reporting across vital sectors of the economy and society. According to the official site, it takes approximately 12 months for the typical NIS2 compliance process, which includes security assessments, auditing, consulting, and tool implementation.

What was missing from the original NIS legislation?

The biggest issue with the original NIS was that it was too broad, too vague, and lacked viable enforcement capabilities. This became obvious during the early days of the COVID pandemic, when many businesses across the EU switched to remote work, greatly increasing the attack surface for most businesses.

When this happened, the following became apparent:

- Cybersecurity resilience of businesses in the EU was ineffective.
- Cybersecurity resilience was inconsistent.

Table of Contents

You might also like:

What is the NIST Cybersecurity

- Understanding of cybersecurity threats was poor.
- There was a severe lack of joint response.
- NIS was not written in a way that considered the implications of rapid digitization.

NIS2 is an attempt to change all of that.

NIS2 aims to address these issues through a more coordinated institutional and regulatory approach, emphasizing the need for a unified response to evolving cybersecurity threats across EU Member States.

Framework? The Ultimate Guide

What are the NIS2 directive requirements?

There are four areas the requirements can be broken into:

- Risk management.
- Corporate accountability.
- Reporting obligations.
- Business continuity.

NIS2 requires organizations to implement ten different baseline security measures, which are:

- Risk assessments and security policies for information systems to enhance cybersecurity capabilities.
- Policies for the use of cryptography and encryption.
- Security around the procurement of systems and their development and operation.
- Security procedures for employees with access to sensitive and important data.
- Policies governing the use of MFA and other authentication solutions.
- Policies and procedures for evaluating the effectiveness of security measures.
- A plan for handling cybersecurity incidents.
- Cybersecurity training and basic computer hygiene.
- A plan for managing business operations during and after a security incident.
- Security around supply chains.

Bitwarden encrypts sensitive data as soon as it's entered in any Bitwarden client. Learn more about how end-to-end encryption paves the way for zero knowledge architecture and why this keeps your information secure.

How an enterprise-wide password manager can help with NIS2 compliance

Given how broad the scope is for NIS2, you might be wondering how a password manager can help with compliance. First, password managers are a cost-effective solution that can be successfully and safely rolled out quickly. On top of that, an enterprise-grade password manager can have an immediate and profound impact on your business security.

With the right password manager, organizations can apply various user types and access controls to ensure the right users can access the correct data (and nothing more). Along with that access control, enterprise-level password managers also include reporting and monitoring tools so those responsible can view detailed events and access logs.

Read more:

How password management helps

With the right password manager, you'll also find integrated two-factor authentication built-in for an added layer of security. But even before that, a solid password manager solution goes a long way to protect against credential attacks. Users will no longer have to memorize or re-use passwords for multiple accounts and can securely share passwords with team members.

The right password manager can help create a culture of security within a business by enabling users to easily and efficiently leverage strong and unique passwords. Credentials that are too long and challenging to memorize are more likely to be secure than passwords created from memory. It's important that businesses choose a password manager capable of living up to the stringent requirements of NIS2. Password managers like Bitwarden offer end-to-end encryption, which lays the groundwork for applications with zero knowledge architectures.

Remember, password managers are an effective means of improving cybersecurity and ensuring compliance with several relevant frameworks, such as ISO/IEC 27001 and ISAE 3402. Password managers can directly help achieve the three major objectives of NIS2 because they directly impact cybersecurity resilience through stronger passwords, reduce inconsistencies in resilience through secure password sharing and using a single, secure platform for password protection, as well as improve situational awareness by encouraging a culture of security by making users aware of how strong passwords — and strong password protection — can prevent incidents.

companies achieve ISO 27001 certification

Meet the NIS2 cybersecurity risk management directive with Bitwarden

Now that NIS2 is national law, your business should already be deep into the compliance process. If your organization falls under the NIS2 directory, you must immediately take steps to determine how to meet the NIS2 requirements. A great place to start with this is by deploying an enterprise-wide password manager to vastly strengthen your organization's security posture in the evolving cybersecurity threat landscape. The right password manager can help prevent credential attacks, give you control over what team members have access to what resources, define roles to make all of this even easier, and monitor activity and events.

Get started today with a free business trial.

FAQs

What is the NIS2?

NIS2 emphasizes cybersecurity risk management processes, which are designed to require businesses to adopt measures to prevent or mitigate cybersecurity threats. It covers risks and measures related to AI, including cybersecurity testing, documentation, and mitigation strategies.

Learn more about Bitwarden security and compliance.

What is the difference between NIST and NIS2?

Unlike NIS2, the NIST Cyber Security Framework does not contain an actionable list. Using a NIST-specific cybersecurity resilience framework can aid organizations in preparing to comply with the information security directive effectively.

What is the NIS2 implementing act?

The NIS2 Directive now encompasses medium and large public and private entities in more critical sectors for cyber resilience.

What is the NIS2 network and information systems?

NIS2, as an EU-wide legislation, emphasizes cybersecurity risk management processes designed to meet the challenge of the evolving cybersecurity threat landscape. The design requires businesses to adopt measures to prevent or mitigate cybersecurity threats. It covers risks and measures related to AI, including cybersecurity testing, documentation, and mitigation strategies.

NIS2 encompasses many more organizations that were not part of the original NIS directive. This includes operators of essential services within critical sectors like healthcare, energy, and transport. The European Union aims to harmonize cybersecurity measures and practices throughout its member states.

It also distinguishes between essential and important entities when setting requirements.