# The NIS2 Directive What to know and how to prepare

# Contents



©2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

# What is NIS2?

## As cybersecurity threats evolve and pose ever-greater risks to individuals and businesses, regulations continuously develop to keep pace with threats and elevate minimum security standards. NIS2 (Network and Information Security version 2), the latest such directive from the European Union, is a significant development in this space.

An expansion and reinforcement of its predecessor, the NIS Directive (2016), NIS2 is a significant overhaul of the EU's cybersecurity regulation landscape, aiming to bolster the overall level of cyber resilience across member states and any entities that do business with them. It extends the scope of the original NIS Directive by broadening the range of sectors and types of entities that fall under its jurisdiction, including those considered to play an 'essential' and 'important' role in the EU's internal market.

For such organizations, NIS2 presents a step up in security compliance — they will either find themselves included under the regulatory scope for the first time or held to much higher standards (and penalties) than under the previous directive.

NIS2 introduces more significant obligations, requiring entities to adopt comprehensive incident reporting mechanisms, robust risk management practices, corporate accountability measures, and effective business continuity strategies. Significantly, the NIS2 Directive also introduces significant consequences for non-compliance, including substantial fines and the potential for litigation.

As an EU Directive, NIS2 will be subject to variances in implementation by member states. This will likely add a layer of complexity for businesses operating across borders within the EU. However, the message is clear: preparation is non-negotiable. Organizations across the EU must take proactive steps to understand the regulation, assess its implications for their operations, and develop an action plan to ensure compliance.

©2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

# Who is Affected by NIS2?

NIS2 significantly expands the scope of regulation beyond its predecessor, casting a much wider net over a range of sectors deemed critical for the EU's international market.

This expansion covers not just sectors considered directly critical but also includes those that are part of the supply chain to these sectors, increasing the number of companies and sectors now falling under regulatory scrutiny.

A key development in NIS2 is the classification of entities into two categories: '**essential**' and '**important**.' This distinction affects the directive's reach and the implications for different types of organizations.

## Essential Entities

This category, also recognized under NIS encompasses sectors foundational to societal and economic well-being. These include transportation, financial services, healthcare and utility companies such as energy suppliers.

For these entities, NIS2 reaffirms their critical status and escalates compliance requirements. For instance, incident reporting must occur within 24 hours — a major update from the previous directive. The most significant change for these companies is the introduction of substantial fines and consequences for non-compliance. So, the rules have changed, and the stakes have never been higher.

**Essential or Critical Infrastructure Industries include:**


©2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

## Important Entities

'Important' entities are a brand new addition to NIS2, meaning the directive will cover these organizations for the first time. Sectors like digital infrastructure, public administration, and manufacturing must quickly adjust and audit their cybersecurity practices.

Given the breadth of the requirements and shorter timeline, this may present a steeper initial challenge. The good news for these entities is that the directive imposes less stringent obligations than organizations classified as 'essential', with lower potential repercussions for non-compliance. However, the need to prepare should not be underestimated.

In short, the NIS2 Directive broadens the regulatory scope, covering more sectors and introducing a classification system that dictates the level of requirements and potential penalties. To understand how to prepare for NIS2, organizations must understand which classification they fall under to know what's expected of them and the possible consequences.

**Important Industries include:**

**Chemical**

**Digital Providers**

**Food**

**Manufacturing**

**Postal Services**

**Research**

**Waste Management**

©2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

# What NIS2 Means for Organizations

Once organizations understand if (and where) they fall under the NIS2 scope, the next step is to gain clarity on the implications of the directive, including the broad organizational requirements, the ten minimum cybersecurity measures, and the specific consequences for non-compliance.

## Introduction of Greater Consequences

The NIS2 Directive introduces far stricter penalties than its predecessor. Minimum fines have been introduced in some places and increased in others. It's worth noting, however, that member states have the discretion to set even higher penalties.

- **Essential Entities**: These organizations face administrative fines of up to €10M or at least 2% of the total annual worldwide turnover in the previous fiscal year of the company to which the entity belongs, whichever is higher.
- **Important Entities**: For these entities, the penalties include administrative fines of up to €7M or at least 1.4% of the total annual worldwide turnover in the previous fiscal year, whichever is higher.

## Broad Organizational Requirements

NIS2 mandates a comprehensive approach to cybersecurity, encompassing a range of organizational responsibilities:

### Duty of Care

Organizations are required to implement robust risk management measures to minimize cyber risks. This includes incident management, securing the supply chain, enhancing network and access control security, and employing encryption where necessary. A key part of this, and one specifically called out in the directive, is ensuring business continuity during significant cyber incidents. This includes system recovery, emergency procedures, and establishing a crisis response team.

### Duty to report

Essential entities are mandated to establish processes for promptly reporting significant security incidents, with specific notification deadlines, such as a 24-hour "early warning" system. NIS2 also significantly emphasises **corporate accountability**, requiring management to be actively involved in and knowledgeable about the organization's cybersecurity measures. Management may face penalties for breaches, including liability and potential temporary bans from management roles.

©2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

## Ten Minimum Measures

### The directive outlines ten minimum cybersecurity measures that organizations must adopt to comply with its requirements:

1. Conduct risk assessments and establish security policies for information systems.
2. Develop policies and procedures to improve the effectiveness of security measures.
3. Implement policies and procedures for the use of cryptography and encryption where relevant.
4. Define a plan for handling security incidents.
5. Ensure security in the procurement, development, and operation of systems, including vulnerability reporting.
6. Provide cybersecurity training and maintain basic computer hygiene practices.
7. Implement security procedures for employees accessing sensitive data, including data access policies and asset management.
8. Manage business operations during and after a security incident, ensuring up-to-date backups and access to IT systems.
9. Utilize multi-factor authentication, continuous authentication solutions, and voice, video, and text encryption.
10. Secure supply chains, assessing vulnerabilities and overall security levels for all suppliers.

While the broad requirements and ten minimum measures give companies a good steer on where to address their policies to prepare for NIS2, as with any regulation, the devil is in the details. Reviewing the directive fully or working with a partner who understands the ins and outs is essential. Crucially, the challenge of tracking the variation across different member states will be pivotal to ensuring compliance, particularly for businesses working across several European countries.

©2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

# Getting the House in Order

Organizations must proactively prepare as the NIS2 Directive takes shape across the European Union. This section outlines the key steps that should be taken.

## Understanding the Directive

As with most business-wide projects, you need to start with a thorough plan and review what you currently have in place and where you need to get to.

**Scope and Classification** — Begin by determining whether NIS2 applies to your organization and, if so, whether you are classified as an "important" or "essential" entity. This will dictate the extent of the requirements you need to meet.

**Review and Audit** — Thoroughly examine the NIS2 requirements and the ten minimum measures. Audit your current cybersecurity posture, processes, and technology against these standards to identify areas needing improvement.

## Gaining Buy-in

IT and compliance teams cannot meet NIS2 requirements on their own. It requires a team effort throughout. From initial planning stages to ongoing review and maintenance, ensure every affected party has a seat at the table.

**Cross-team collaboration** — Implementing the required security measures and processes demands collaboration and buy-in from all levels of the organization. Leadership backing is crucial for initiating change and because NIS2 mandates

©2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

corporate management's responsibility for cybersecurity. IT, security, and operations teams must also work together to implement security, backup, and encryption measures effectively.

**Organizational Training** — Beyond leadership, adherence to NIS2 involves training the organization to update security practices in line with minimum measure 6. It's crucial that this training isn't a one-time action, but a continuous process that helps maintain awareness of responsibilities long-term, evolves over time, and onboards new employees effectively.

## Duty of Care

Meeting the requirements of NIS2's 'duty of care' requires a thorough audit of security risk across the organization. This includes data storage, data access, security and vulnerability scanning.

**Data Management and Hygiene** — Ensure good data management practices, such as data tagging, appropriate data locality, secure storage and backups. Extending the duty of care to backups is also important. This includes having immutable backups (which can't be targeted or changed by attacks like ransomware) and keeping multiple copies of data in case of errors.

**Security Measures** — Continuously evaluate and ensure appropriate security measures are in place, especially for personnel accessing sensitive or important data. Incorporate zero-trust frameworks, cryptography, and encryption, and ensure all systems (third-party and first-party) are secure and regularly scanned for vulnerabilities. Implement robust security measures for supply chain vendors and enforce multi-factor authentication where appropriate.

## Incident Response

NIS2 mandates having a comprehensive plan for security incidents that includes maintaining operations and continuity during and after an incident. Therefore, businesses need to have a dedicated incident response team including stakeholders across different business units to define and regularly drill a robust incident response process.

**Threat Detection** — Early detection of incidents, such as ransomware attacks that may breach systems well in advance, is critical. Invest in threat detection capabilities, monitoring, alerts, and malware detection to catch incidents as early as possible.

**Backup Strategy** — Ensure up-to-date backups are in place, focusing on mission-critical data. It is recommended to follow the Veeam 3-2-1-1-0 Golden Backup Rule. This includes having three copies of data on two different media, with one copy offsite and one to be air-gapped, immutable, or offline, and aiming for zero errors in backup and recovery verification.

**Response and Recovery** — Develop processes for incident reporting and communication during an incident. For recovery, have disaster recovery processes in place to ensure business continuity. Reliable backups are crucial, but a robust recovery process that includes planning for recovery in a separate, secure environment is vital to minimize downtime and its associated costs.

**Strategic Planning for Recovery Environments** — It is crucial that organizations consider their recovery environments. Often, you cannot recover in the same environment where the incident occurred. Planning for a separate, secure recovery environment in advance is essential. For example, the middle of a security incident is not the time to integrate with a new cloud provider for the first time!

©2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

# Navigating NIS2 with Veeam

**As the European Union introduces the NIS2 Directive, businesses across various sectors need to bolster their cybersecurity and resilience practices.**

Wherever businesses fall under the directive's scope, preparing for it will be a fresh challenge — 'Important' entities are navigating these waters for the first time. In contrast, 'essential' entities must meet even stricter requirements than before. Despite the variance in the execution of details and requirements by different EU member states, the overarching principles of NIS2 are consistent enough for organizations to begin preparing now.

While it's easy to view this kind of regulatory obligation as an inconvenience or burden, organizations should embrace it. The practices and requirements defined in NIS2 are essential for protecting businesses from scaling cyber threats — companies need to be moving towards these practices if they are not already part of their security posture.

©2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

## How Veeam Can Help

Meeting NIS2 requirements is an organization-wide, top-to-bottom mission. For many businesses, this will require implementing a host of new processes and technologies.

While not a silver bullet, the Veeam Data Platform is well-positioned to help entities meet various NIS2 requirements, particularly around data hygiene, reporting and auditing, data backup and disaster recovery. The Veeam Data Platform includes Veeam Backup & Replication, Veeam Recovery Orchestrator, and Veeam ONE for Monitoring and Alerting, offering a robust foundation for securing digital assets and boosting cyber resilience.

- **Veeam Backup & Replication:** Secures data against loss and threats by providing reliable backup and replication for all workloads.
- **Veeam Recovery Orchestrator:** Ensures the rapid recovery of critical services with automated disaster recovery, planning and testing.
- **VeeamONE:** Provides advanced monitoring, reporting, and capacity planning for your Veeam backup environment, enhancing your ability to maintain business continuity and meet compliance requirements.
- **Veeam Security & Compliance Analyzer:** Ensures successful recovery with automated scans, leveraging infrastructure hardening and data protection best practices
- **Veeam Threat Center:** Highlights threats, identify risks and measure the security score of your environment


Veeam's solutions are designed to be a vital part of your cybersecurity toolbox, helping your organization navigate the complexities of NIS2 compliance. However, preparation for NIS2 extends beyond the capabilities of any single provider. It involves a commitment to ongoing cybersecurity education, the adoption of best practices, and the willingness to invest in the necessary technologies and processes to protect against evolving threats.

Speak with a Veeam expert today to understand how Veeam can help your organization become NIS2-ready. Discover how Veeam's data protection and management solutions can fortify your cybersecurity posture, ensure compliance with NIS2, and safeguard your organization's future in the face of emerging cyber threats.

©2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

veeam

# Want to Learn More?

Start your journey to NIS2 compliance today. Talk to us about how Veeam solutions can put cybersecurity at the centre of your business.

Alternatively visit our NIS2 landing page for more detail

LET'S TALK

LEARN MORE