OBJECT FIRST

White Paper

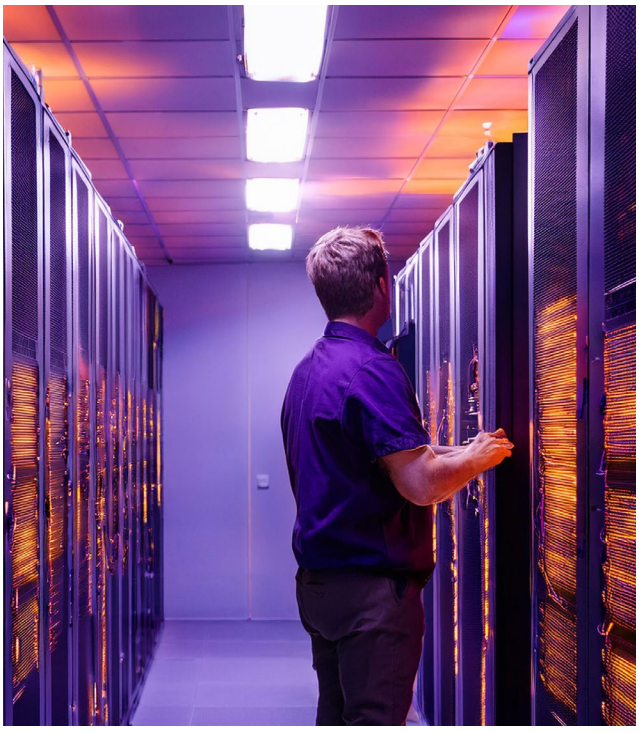
New NIS2 Directive

Essential Facts and How to Comply

NIS2 Primer

As digital threats have increased in frequency and cyber attackers evolved in sophistication, governments and international agencies are proposing new and updated regulations to increase resilience. When a new regulation is introduced, it can be challenging to learn, unpack, and implement it before the start date.

If you work in IT in the European Union (EU), you are already aware that unlocking the details of Network and Information Security Directive 2 (NIS2) is in your future. We thought it might be helpful to give you a quick primer on NIS2 to jump-start your implementation journey so you stay ahead of the regulations and, most importantly, ahead of attackers.



What is NIS2?

The Network and Information Security Directive 2 (NIS2) aims to bolster cybersecurity across the EU Member States and any entities that do business with them. It responds to the increasing threats associated with digitalization and the rise in cyber attacks.

NIS2 extends the scope of the original NIS Directive with more sectors and types of entities that fall under its jurisdiction, including those believed to have an 'essential' and 'important' role in the EU's internal market. It introduces more significant requirements, including comprehensive incident reporting, risk management practices, corporate accountability measures, and business continuity strategies.

Risks of Non-Compliance

The NIS2 Directive includes substantial fines for non-compliance, as well as the potential for litigation. NIS2 mandates member states to put these requirements into national law by October 17, 2024. While implementation may vary slightly, thorough preparation for that deadline is essential.

You must proactively understand the directive, identify the impacts on your organization, and establish your plan to reach compliance.

At this point, you are probably wondering: 'How does it impact me?' but first, you must understand who 'you' are and whether NIS2 impacts your organization.

Am I Essential or Important?

NIS2 categorizes business organizations into two groups: 'essential' and 'important.' Where you fall in this grouping will help you understand how NIS2 will impact your organization moving forward.

Essential Entities

NIS2 identifies crucial sectors like transportation, financial services, healthcare, and utility companies (including energy suppliers) as 'essential entities', underscoring their importance to societal and economic well-being. It elevates their compliance obligations, notably mandating incident reports within 24 hours — a significant tightening of requirements from the earlier directive. Additionally, it introduces hefty fines and severe consequences for failing to comply, emphasizing the increased stakes and stricter regulatory landscape these entities now face.

You are an essential entity If your business has over 250 employees and an annual turnover of € 50 million and falls under one of these categories:

- Digital Infrastructure
- Energy
- Finance
- Health
- Public Administration
- Space
- Transport
- Water supply (drinking & wastewater)

Important Entities

NIS2 introduces a new classification for 'important' entities, broadening the directive's scope to encompass sectors like postal services, waste management, and manufacturing for the first time. This expansion means these sectors must rapidly evaluate and enhance their cybersecurity measures to comply with NIS2. Although 'important' entities face less severe obligations and penalties for non-compliance than their 'essential' counterparts, the challenge of meeting these requirements within a relatively short timeframe should not be underestimated.

You are an 'important' entity if your business has over 50 employees and an annual turnover of € 10 million and falls under one of these categories (this also includes the categories listed as essential):

- Chemicals
- Foods
- Manufacturing
- Postal Services
- Research
- Waste Management

How NIS2 Impacts You

If your business falls within the 'essential' or 'important' categories listed, your next step is understanding what NIS2 means for your organization and how it can impact you.

Getting Started

The NIS2 Directive emphasizes a thorough strategy for cybersecurity within organizations. While it is a very detailed regulation framework, and we recommend that impacted organizations within a Member State take the time to read the articles for themselves, we created some highlights to help you begin your evaluation, starting with ten minimum cybersecurity measures highlighted in the Directive.

The Ten Cybersecurity Risk-Management Measures

One of the most critical sections of the directive is Article 21, which lists ten cybersecurity risk-management measures. Member States must ensure that 'essential' and 'important' entities implement suitable technical, operational, and organizational measures to manage risks to the security of their network and information systems used in their operations or services. These measures should prevent or minimize the impact of incidents on service recipients. They must consider the latest technology, relevant standards, and costs and ensure the security level is appropriate for the risk level. When assessing the proportionality of security measures, organizations must consider their risk exposure, size, and the potential impact of incidents. This includes evaluating the severity and likelihood of incidents and their societal and economic effects.

The NIS2 directive lists ten cybersecurity measures that all qualifying entities must implement:

1. Policies on risk analysis and information system security
2. Incident handling
3. Business continuity processes, such as backup management, disaster recovery, and crisis management
4. Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
5. Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
7. Basic cyber hygiene practices and cybersecurity training
8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption
9. Human resources security, access control policies, and asset management
10. Multi-factor authentication or continuous authentication solutions, secured voice, video, and text communications, and secured emergency communication systems within the entity, where appropriate.

Duty to Report

A recurring theme throughout the entire NIS2 directive is the importance of reporting. 'Essential' entities are mandated to set up procedures for quickly reporting significant cybersecurity incidents, with specific deadlines for reporting, including a preliminary 24-hour 'early warning' system.

NIS2 also highlights the importance of corporate responsibility, requiring that management actively engage with and understand the organization's cybersecurity efforts. Managers could be penalized for security breaches, potentially facing liabilities and even temporary prohibitions from managerial positions.

Penalties

The new rules under the NIS2 Directive are much more demanding than before, introducing higher or entirely new fines in some cases.

However, countries within the Union can decide on even higher fines if they choose. Businesses considered 'essential' must be prepared to face fines up to €10 million or 2% of their global yearly earnings from the last year, whichever amount is higher. Businesses considered 'important' could see fines up to €7 million or 1.4% of their global earnings from the previous year, again whichever is higher.

But Wait, There is More

These three sections showcase a broad range of the expectations in the NIS2 directive; however, this is not all-encompassing. We encourage every business operating within the European Union to review the entire directive and its requirements with their teams and fully understand the expectations and ramifications of this massive legislation.

How Object First Can Help

NIS2 is a tremendously important evolution in security regulation and could be a significant lift to ensure compliance in the data center of 'important' and 'essential' entities. In addition to writing this primer, we thought we'd extend some of our recommendations to help ensure you achieve your NIS2 goals efficiently.

Zero Trust Data Resilience

Section 89 of the introduction of the NIS2 directive mentions organizations adopting Zero Trust to help improve their overall security posture. Zero Trust is an essential set of principles to ensure the security of production apps and infrastructure. Still, it does not consider Backup Software and Backup Storage as part of its overall maturity model.

Last year, Veeam and Numberline published their research on Zero Trust Data Resilience (ZTDR).
It is a comprehensive data protection approach that expands Zero Trust security principles to an organization's backup environment. It introduces critical elements such as separating Backup Software and Backup Storage, multiple resilience zones, and immutable and encrypted backup storage. This approach minimizes risk, fortifies data protection, and increases an organization's security posture. Understanding ZTDR is crucial for organizations as it provides a robust framework to safeguard their data against cyber threats, particularly ransomware and data exfiltration attacks. It offers a more secure alternative to traditional security models regarding data protection and should be part of every admin checklist regarding their NIS2 preparation. For more information about ZTDR, please read our whitepaper.

Read the Whitepaper

Immutable Backup Data Storage

Surprisingly, the word immutability is not mentioned in the NIS2 directive. The most important part of data protection is the ability to recover; with immutable storage, the likelihood of recovery is much higher. Most attacks today target the backup infrastructure first to eliminate the possibility of recovery and ensure ransom payment.

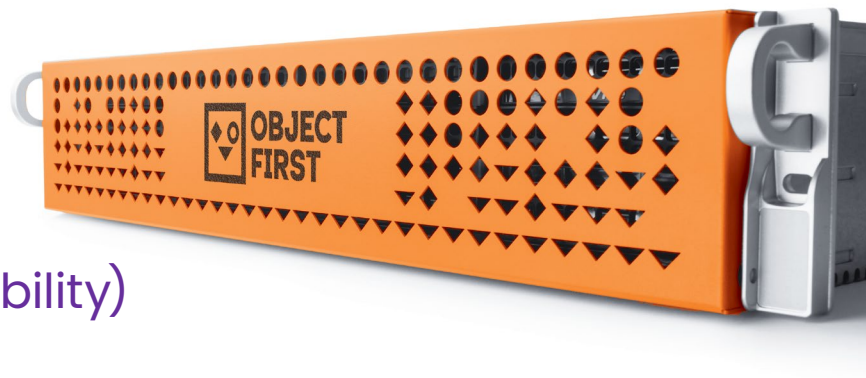
The previously mentioned Article 21's cybersecurity measures directly mention data protection requirements, cybersecurity hygiene, and encryption. Still, all of these can be breached and destroyed. In contrast, an immutable storage target that complies with ZTDR best practices like zero access to root, an inherently segmented architecture from the backup software, and storage that leverages S3 object lock in compliance mode will help increase resilience in the face of an attack.

Achieving Recovery Time Objectives

The directive makes numerous statements about the importance of a recovery strategy, including a responsive recovery plan and testing recovery simulations before a cyberattack occurs. We recommend that all organizations impacted by the NIS2 legislation take the time to evaluate their current data protection environments and run through test recovery scenarios to better gauge their true recovery point objectives (RPO) and recovery time objectives (RTO). Understanding how far back you may have to go to recover, in conjunction with how long it will take to get the data back, is a crucial part of the responsiveness that NIS2 demands.

Meet Ootbi

(Out-of-the-box Immutability)



Object First seeks to help all Veeam customers in the EU ensure that their backup storage exceeds NIS2 standards. That's why Object First created Ootbi, the best storage for Veeam. Ransomware-proof and immutable out-of-the-box, Ootbi by Object First delivers secure, simple, and powerful backup storage that is purpose-built for Veeam. The appliance can be racked, stacked, and powered in 15 minutes.

Ootbi helps Veeam admins implement a Zero Trust Data Resilience architecture for unbreakable backup and recovery. With its secure-by-design architecture, Ootbi ensures Veeam backup data stays immutable and requires no additional security expertise from the end user.

Conclusion

The NIS2 directive is coming soon; on October 17, 2024, the directive will be adopted into law by member states. As with any major mandate, this will require significant effort from many individuals within 'important' and 'essential' organizations to ensure they are not fined for non-compliance. Education will always be a critical first step in meeting the demands of legislation like these. Please take the time to read the entire NIS2 directive if you are impacted by it and ensure your organization is aware of the implications. While this initiative may be disruptive initially, decreasing disruptive criminal activity will be well worth the effort.

OBJECT FIRST

objectfirst.com ↗

All links from this document can be found here: