OBJECT FIRST

Checklist

NIS2 Compliance: Your 8-Step Checklist

July, 2026

The Network and Information Security Directive 2 (NIS2) took effect in the EU on October 17, 2024. It introduced new obligations to strengthen cybersecurity, audit regularly, and report incidents swiftly or face penalties. National transposition is now well underway across Member States, with enforcement accelerating. Compliance is mandatory for organisations providing essential services—but also vital for those competing to be their suppliers.

This Object First NIS2 checklist is designed to help you navigate the compliance process and protect your operations from cyberthreats. You and your organisation can become Simply Resilient with the ultimate ransomware defence.

Please note that this checklist is intended only as a guide and is not all-inclusive. Reviewing the full directive in detail is essential to ensure you understand your obligations.

Get Ready

1. Understand Your Classification and Jurisdiction

Determining whether your organisation is classified as 'essential' or 'important' under NIS2 is crucial, as it defines the specific compliance requirements you must meet. Organisations should also check transposition law in every jurisdiction they operate in, as individual Member States may impose stricter requirements than the EU baseline.

Action Items:

- [ ] Identify if your organisation falls under the 'essential' or 'important' category, whether due to category or size
- [ ] Review NIS2 requirements specific to your classification
- [ ] Communicate classification status and obligations to relevant stakeholders

2. Conduct a Comprehensive Risk Analysis

NIS2 mandates that organisations must conduct a thorough risk analysis to identify vulnerabilities in their information systems and networks.

Action Items:

- [ ] Perform a detailed risk assessment of all IT systems, networks, and software supply chains
- [ ] Document potential vulnerabilities, including risks from third-party vendors and the software supply chain
- [ ] Develop mitigation strategies to secure privileged accounts, implement least-privilege access

3. Establish Incident Handling and Reporting Procedures

Under NIS2, timely incident reporting follows a staged sequence. You must send an early warning within 24 hours of becoming aware of a significant incident, follow with a fuller notification within 72 hours, and submit a final report within one month.

Action Items:

- [ ] Document procedures for each potential reporting stage—early warning, notification, and final report—with clear ownership and deadlines for each
- [ ] Train staff on incident reporting procedures, including recognising and reporting phishing attempts
- [ ] Ensure reporting systems are tested and functioning, with emphasis on securing sensitive data during reporting

4. Implement a Zero Trust Strategy

Traditional perimeter-based security architectures aren't suited to today's borderless world of cloud services and hybrid workforces. NIS2 emphasises adopting Zero Trust principles to enhance security. While Zero Trust minimises the attack surface and assumes breaches, Zero Trust Data Resilience (ZTDR) extends these principles to data backup and recovery environments, protecting them against ransomware and data exfiltration.

Action Items:

- ☐ Apply Zero Trust principles across your data protection infrastructure, ensuring continuous authentication and threat analytics
- ☐ Separate backup software and storage; use multiple resilience zones with least privilege access
- ☐ Include policies for cryptography, encryption, and multi-factor authentication (MFA)

5. Establish Absolutely Immutable Backup Data Storage

Absolute Immutability means that even the most privileged admin or attacker with access to backup storage cannot modify or delete data.

Action Items:

- ☐ Deploy immutable storage solutions that support compliance with Article 21's cybersecurity measures
- ☐ Utilise S3 object lock in compliance mode to enhance data resilience
- ☐ Communicate classification status and obligations to relevant stakeholders

6. Meet Recovery Time Objectives (RTO)

The NIS2 directive stresses the importance of having a robust recovery and business continuity strategy. Meeting Recovery Time Objectives (RTO) is essential to ensure your data can be restored quickly during a cyberattack.

Action Items:

- ☐ Define and document your organisation's RTOs for critical systems
- ☐ Test recovery plans regularly to ensure they meet RTO targets and align with Zero Trust principles
- ☐ Adjust your recovery strategies to meet NIS2 requirements and business continuity objectives, including rapid recovery from ransomware attacks

7. Establish Board-Level Governance

NIS2 places cybersecurity governance directly with senior management. Management bodies must approve cybersecurity risk-management measures, oversee their implementation, and maintain the knowledge to do so effectively. Where this falls short, regulators can act directly against individuals responsible.

Action Items:

- [ ] Ensure the management body formally approves and oversees cybersecurity risk-management measures
- [ ] Provide training so management can identify and assess cyber risks and judge the adequacy of existing measures
- [ ] Keep board minutes, training records, and approval trails as evidence of board-level governance

8. Ensure Continuous Compliance Monitoring

NIS2 compliance is an ongoing process requiring continuous monitoring and updates as threats evolve.

Action Items:

- [ ] Set up a compliance monitoring system to track adherence to NIS2 requirements
- [ ] Schedule regular audits and reviews of cybersecurity practices, including the security of the software supply chain
- [ ] Update policies and procedures in response to new threats, regulatory changes, and advancements in Zero Trust strategies

Zero Trust and Enterprise Data Backup

The Zero Trust model represents the best practices for organisations seeking to protect and secure their data and business. However, this model has not been substantively applied to data backup and recovery—until now.

Zero Trust Data Resilience (ZTDR) is a new model that extends the principles of Zero Trust to address the data backup and recovery use case.

Learn more about Zero Trust and how it applies to backup and recovery infrastructure, ZTDR principles and architecture, and how to ransomware-proof your backup infrastructure and storage.

Read the White Paper →

Stay Ahead With the Object First NIS2 White Paper

Download our comprehensive NIS2 white paper for a more detailed understanding of the requirements and actionable insights to secure your organisation against evolving cyber threats.

You will learn:

- Key requirements and obligations under the NIS2 Directive.
- Practical steps to enhance your organisation's cybersecurity and compliance efforts.
- Strategies to ensure you and your organisation become Simply Resilient.

Ready to learn more?

Download the White Paper → **Contact Sales →**

OBJECT FIRST

Simply Resilient for Veeam

Contact Us →