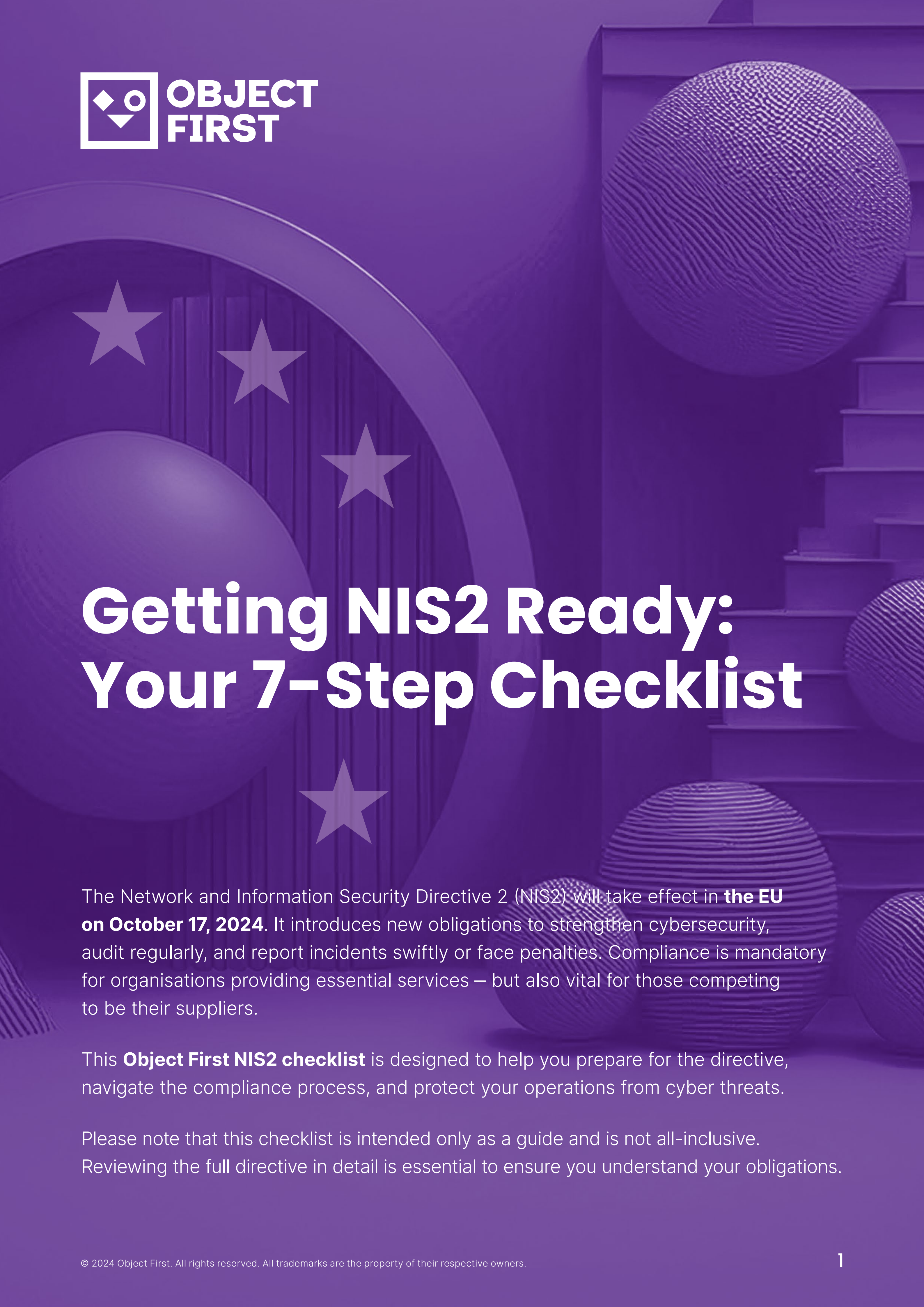


Getting NIS2 Ready: Your 7-Step Checklist

The Network and Information Security Directive 2 (NIS2) will take effect in **the EU on October 17, 2024**. It introduces new obligations to strengthen cybersecurity, audit regularly, and report incidents swiftly or face penalties. 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 prepare for the directive, navigate the compliance process, and protect your operations from cyber threats.

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.

© 2024 Object First. All rights reserved. All trademarks are the property of their respective owners.

Get Ready

1. Understand Your Classification

Determining whether your organization is classified as “Essential” or “Important” under NIS2 is crucial, as it defines the specific compliance requirements you must meet.

Action Items:

□ Identify if your organization falls under the “Essential” or “Important” category.

□ Review NIS2 requirements specific to your classification.

□ Communicate classification status and obligations to relevant stakeholders.

2. Conduct a Comprehensive Risk Analysis

NIS2 mandates that organizations 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.

□ Prioritize handling discovered risks and develop mitigation strategies to secure privileged accounts and mplement least privilege access.

3. Establish Incident Handling and Reporting Procedures

Under NIS2, timely incident reporting is critical. Initial reports must be submitted within 24 hours of detection.

Action Items:

□ Create a protocol for immediate incident detection, handling, and reporting.

□ Train staff on incident reporting procedures, including recognizing 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 emphasizes adopting Zero Trust principles to enhance security. While Zero Trust minimizes 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).

© 2024 Object First. All rights reserved. All trademarks are the property of their respective owners.

5. Establish Immutable Backup Data Storage

Ensuring that your backup data is immutable is crucial for recovery and a key tenant of the previously mentioned ZTDR strategy. Immutable storage ensures that backups cannot be altered or deleted by ransomware.

Action Items:

- □ Deploy immutable storage solutions that support compliance with Article 21's cybersecurity measures.
- □ Utilize S3 object lock in compliance mode to enhance data resilience.
- □ Regularly review and test your backup infrastructure to ensure immutability and quick recovery times (RTO).

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 organization'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. 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.

© 2024 Object First. All rights reserved. All trademarks are the property of their respective owners.

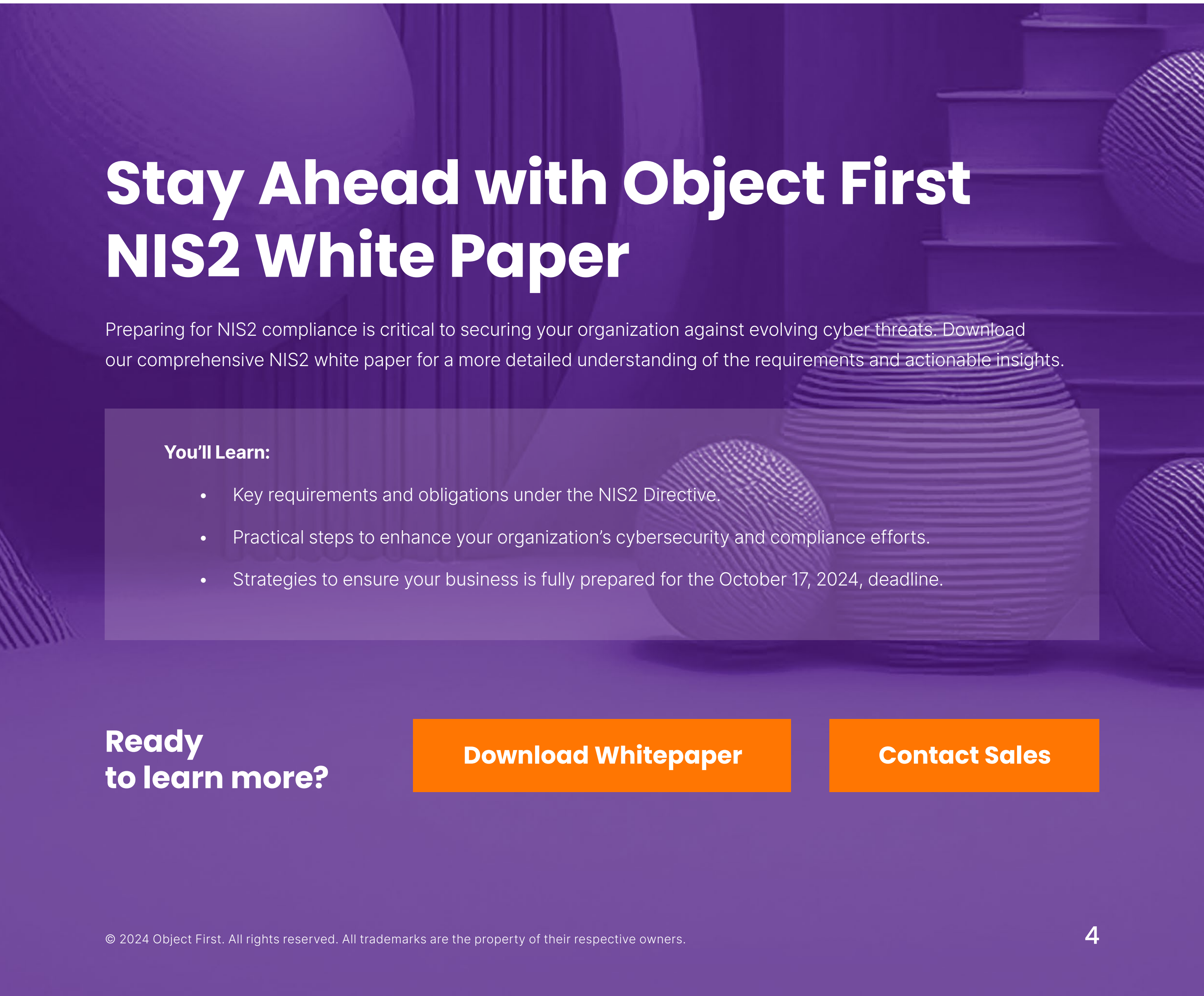
Zero Trust and Enterprise Data Backup

The Zero Trust model represents the best practices for organizations 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, Zero Trust Data Resilience (ZTDR) principles and architecture, and how to ransomware-proof your backup infrastructure and storage.

Read the Whitepaper



Stay Ahead with Object First NIS2 White Paper

Preparing for NIS2 compliance is critical to securing your organization against evolving cyber threats. Download our comprehensive NIS2 white paper for a more detailed understanding of the requirements and actionable insights.

You'll Learn:

- Key requirements and obligations under the NIS2 Directive.
- Practical steps to enhance your organization's cybersecurity and compliance efforts.
- Strategies to ensure your business is fully prepared for the October 17, 2024, deadline.

Ready to learn more?

Download Whitepaper

Contact Sales

© 2024 Object First. All rights reserved. All trademarks are the property of their respective owners.