Lansweeper

NIS2 READINESS CHECKLIST

Learn how to Achieve NIS2® Compliance

NIS2 READINESS CHECKLIST

The NIS2 Directive provides legal measures to boost the overall level of cybersecurity in the European Union. Compliance is crucial - and mandatory - for organizations operating within the EU or providing services to EU member states. NIS2 introduces significant changes, broadening the scope of compliance and imposing stringent measures to enhance your overall security posture.

This 10-step checklist serves as a roadmap to prepare you for the NIS2 directive. From understanding the scope and conducting risk assessments to implementation. This checklist not only helps in preparing for the October 17, 2024 deadline but also establishes a foundation for sustained cybersecurity resilience, fostering a proactive and adaptive security posture in the face of an ever-changing threat landscape.

NIS2 READINESS CHECKLIST

STEP 1

Understand the NIS2 Scope:

- [ ] Identify whether your organization falls within the scope of NIS2, considering both sector and size criteria.

STEP 2

Policies for Risk Analysis and Information System Security

- [ ] Develop and document comprehensive policies for risk analysis and information system security.
- [ ] Ensure your policies encompass identification, assessment, and mitigation of cybersecurity risks.
- [ ] Use Lansweeper's discovery capabilities to identify potential security risks within your IT infrastructure.
- [ ] Leverage Lansweeper's risk insights to prioritize and mitigate cybersecurity vulnerabilities effectively.

STEP 3

Incident Handling

- [ ] Establish protocols and procedures for handling cybersecurity incidents promptly and effectively.
- [ ] Define roles and responsibilities within the incident response team.
- [ ] Establish incident communication channels.
- [ ] Use Lansweeper to swiftly identify vulnerable machines and prioritize remediation efforts during cybersecurity incidents
- [ ] Use detailed asset data for post-remediation investigations.

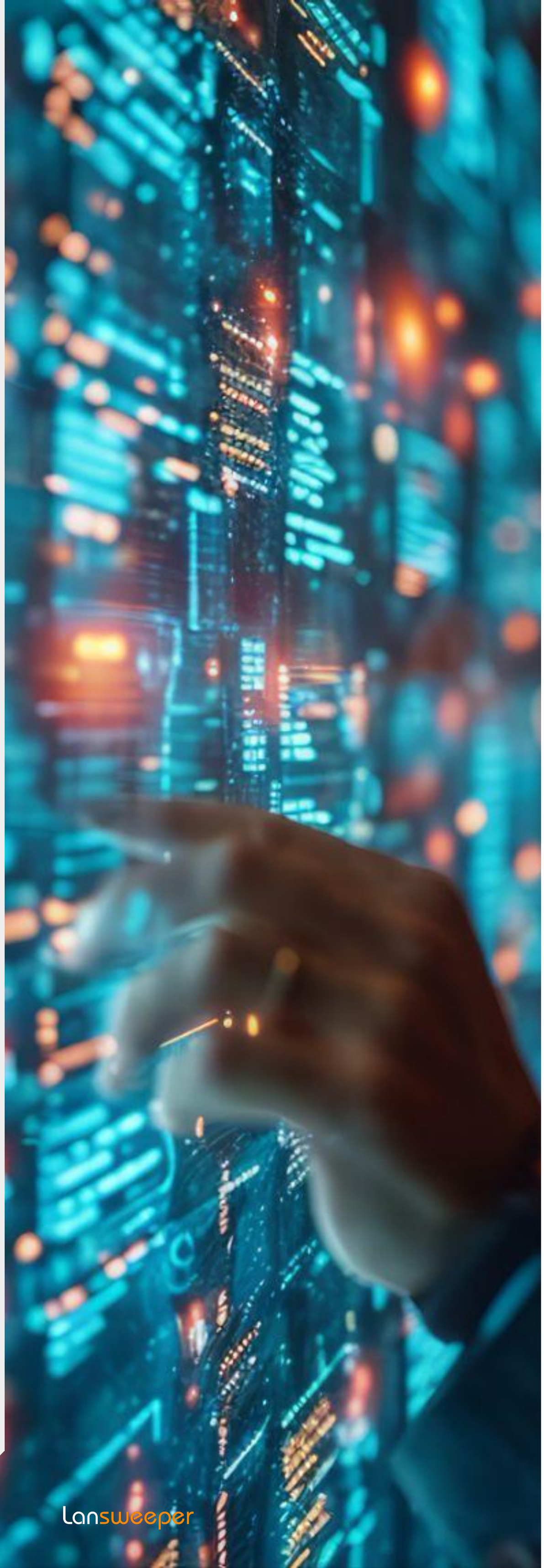
How Lansweeper helps with NIS2 Compliance

Learn More

Try Lansweeper for Free

- 2 weeks of unlimited scanning
- No card required
- Sign up now & start when ready
- Access all features
- 5-minute onboarding

Try Now



NIS2 READINESS CHECKLIST

STEP 4

Business Continuity, Backup Management, and Disaster Recovery

- [ ] Implement robust business continuity plans, including backup management and disaster recovery strategies.

- [ ] Maintain an inventory of backup agents and versions using Lansweeper to ensure continuity of backup and disaster recovery services

STEP 5

Supply Chain Security

- [ ] Assess third-party suppliers and service providers to mitigate any security risks in your supply chain.

- [ ] Establish security-related requirements and expectations in contracts with suppliers.

STEP 6

Assessment of Cybersecurity Risk-Management Measures

- [ ] Develop procedures to assess the effectiveness of cybersecurity risk-management measures regularly.

- [ ] Conduct periodic audits and evaluations to identify areas for improvement and ensure compliance.

NIS2 READINESS CHECKLIST

STEP 7

Basic Cyber Hygiene Practices and Cybersecurity Training

- [ ] Promote basic cyber hygiene practices among staff, including password management and phishing awareness.
- [ ] Provide cybersecurity training and awareness programs to enhance staff's ability to recognize and respond to security threats.
- [ ] Monitor cybersecurity hygiene practices, such as software updates and encryption usage, using Lansweeper's reporting capabilities.

STEP 8

Policies and Procedures Regarding the Use of Cryptography

- [ ] Establish policies and procedures governing the use of cryptography to protect sensitive information.
- [ ] Ensure encryption protocols align with industry standards and regulatory requirements.
- [ ] Monitor encryption status and implementation across your environment using Lansweeper's discovery and reporting.

STEP 9

Human Resources Security, Access Control Policies, and Asset Management

- [ ] Implement access control policies to manage user permissions and privileges effectively.
- [ ] Maintain accurate inventories of IT assets and devices, including hardware, software, and data.
- [ ] Use Lansweeper to get a full inventory of all devices and their users in your environment, including user privileges, to ensure you adhere to access control policies.

STEP 10

Use of Multi-Factor Authentication (MFA) and Secured Communications

- [ ] Implement multi-factor authentication (MFA) or continuous authentication solutions to enhance access security.
- [ ] Secure voice, video, and text communications within the organization to protect sensitive information.

Lansweeper

Lansweeper is an IT asset management software provider helping businesses better understand, manage and protect their IT devices and network. Lansweeper helps customers minimize risks and optimize their IT assets by providing actionable insight into their IT infrastructure at all times, offering trustworthy, valuable, and accurate insights about the state of users, devices, and software.

Since its launch in 2004, Lansweeper has been developing a software platform that scans and inventories all types of IT devices, installed software, and active users on a network - allowing organizations to centrally manage their IT.

The Lansweeper platform currently discovers and monitors over 80 million connected devices from 28,000+ customers, including Mercedes, FC Barcelona, Michelin, Carlsberg, Nestle, IBM, and Samsung to governments, banks, NGOs, and universities, driven by its 150+ strong teams in Belgium, Spain, Italy, the UK and the USA.

🔥

Want to try Lansweeper now?

Start Your Free 14-day Trial

👁️

Not ready yet?

Watch the demo video