Lansweeper

NIS2 READINESS CHECKLIST

Learn how to Achieve NIS2® Compliance

September 2024

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 and Applicability

- [ ] Identify whether your organization falls within the scope of NIS2 , considering both sector and size criteria. Use this guide as a reference

- [ ] Assess which parts of your operations are within the scope of NIS2 based on your sector and size.

STEP 2

Conduct a Risk Assessment

- [ ] Identify and document all vulnerabilities within your IT infrastructure.

- [ ] Assess the potential risks and impacts associated with each vulnerability.

- [ ] Develop and implement a risk management strategy that prioritizes the most critical risks.

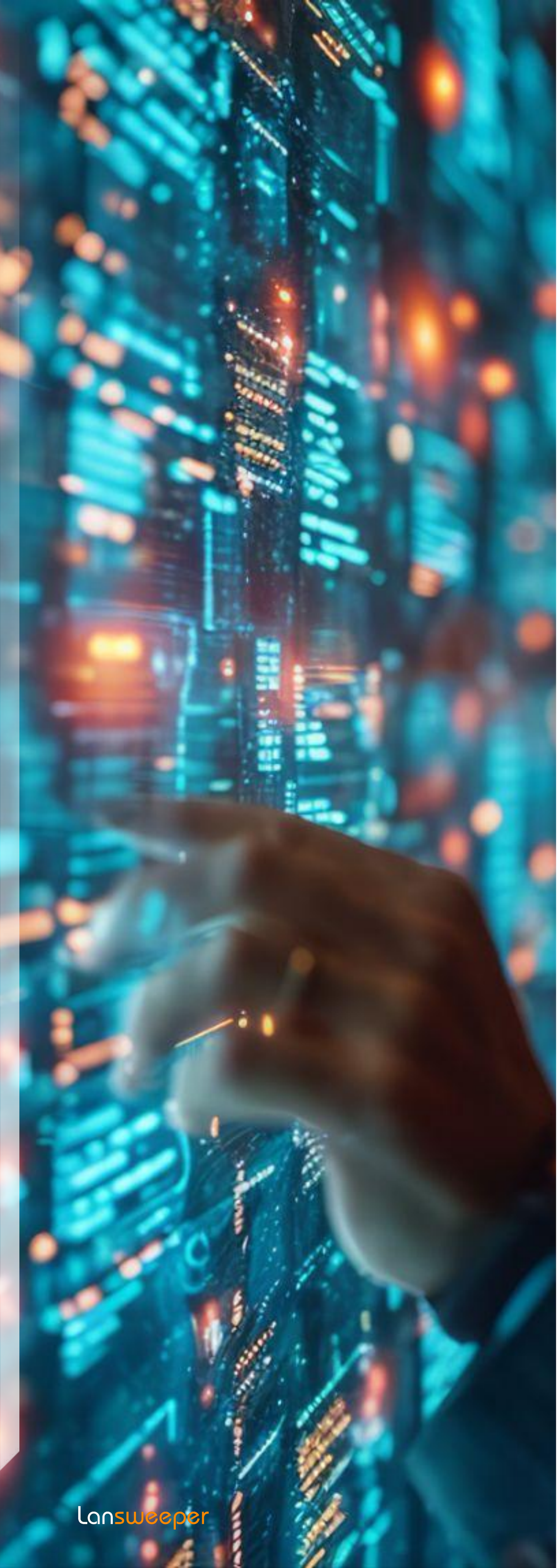
STEP 3

Implement Security Measures

- [ ] Ensure all IT systems and networks are equipped with up-to-date antivirus, anti-malware, and encryption software.

- [ ] Implement multi-factor authentication (MFA) for accessing critical systems and data.

- [ ] Establish a process to regularly update and patch all software and systems to close security gaps.



STEP 4

Establish Incident Response Procedures

- [ ] Develop and document a comprehensive incident response plan.
- [ ] Define what constitutes a security incident and the appropriate escalation paths.
- [ ] Assign roles and responsibilities for incident management to specific personnel or teams.
- [ ] Ensure regular training and drills are conducted to test the effectiveness of the incident response plan.

STEP 5

Ensure Business Continuity and Crisis Management

- [ ] Develop and regularly update backup management and disaster recovery plans.
- [ ] Ensure that all critical data is regularly backed up and that backup systems are tested for reliability.
- [ ] Implement crisis management procedures to maintain operations during and after a cyber incident.

STEP 6

Secure the Supply Chain

- [ ] Assess the cybersecurity posture of all third-party suppliers and service providers.
- [ ] Require suppliers to comply with your organization’s security policies and NIS2 requirements.
- [ ] Establish contracts that clearly define the security responsibilities of each supplier.

STEP 7

Regular Monitoring and Updating

- [ ] Continuously monitor your IT environment for new vulnerabilities, threats, or anomalies.
- [ ] Keep all systems, software, and security tools up-to-date to protect against emerging threats.
- [ ] Use automated tools to regularly scan and update your security measures.

STEP 8

Implement Cyber Hygiene Practices and Training

- [ ] Ensure that all employees receive regular cybersecurity training and are aware of best practices.
- [ ] Monitor compliance with basic cyber hygiene practices, such as the use of strong passwords, regular software updates, and secure handling of sensitive information.

STEP 9

Document and Report Compliance Efforts

- [ ] Keep detailed records of all cybersecurity policies, risk assessments, and incident response activities.
- [ ] Generate regular compliance reports to demonstrate adherence to NIS2 requirements.
- [ ] Prepare for audits by ensuring that all documentation is complete, accurate, and up-to-date.

STEP 10

Review and Improve

- [ ] Conduct periodic audits and assessments to identify areas for improvement and implement corrective actions.
- [ ] Regularly review and update your cybersecurity policies and procedures to reflect changes in the threat landscape or regulatory requirements.
- [ ] Engage in continuous learning to stay informed about new cybersecurity trends, threats, and best practices.

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