

### **NIS2 Compliance Checklist**

#### **Introduction**

The NIS2 Directive is a cornerstone regulation aimed at strengthening cybersecurity across critical sectors in the European Union. It places greater accountability on organizations to manage cyber risks, secure supply chains, and report incidents.

This comprehensive checklist provides actionable steps to ensure your organization meets NIS2 requirements. Whether you are just beginning your compliance journey or looking for a quick review, this resource will guide you through the essential aspects of NIS2 compliance.

#### **Purpose**

This checklist is designed to help organizations navigate the requirements of the NIS2 Directive, ensuring they take the necessary steps to bolster their cybersecurity posture. By following this checklist, your organization can align with NIS2 standards, protect critical infrastructure, and avoid potential penalties for non-compliance.

### **Checklist**

#### **1. Governance and Leadership**

* DoneIdentify key stakeholders responsible for NIS2 compliance.
* DoneAppoint a Chief Information Security Officer (CISO) or equivalent.
* DoneEstablish clear communication lines for cybersecurity incidents.
* DoneEnsure board-level awareness and involvement in cybersecurity strategies.

#### **2. Risk Management and Security Measures**

* DoneConduct a comprehensive cybersecurity risk assessment.
* DoneImplement a risk management framework aligned with NIS2 requirements.
* DoneApply technical and organizational measures to mitigate risks.
* DoneEnsure secure system design and continuous system monitoring.
* DonePerform regular penetration testing and vulnerability assessments.

#### **3. Supply Chain Security**

* DoneIdentify critical third-party suppliers and partners.
* DoneAssess the cybersecurity posture of all vendors and service providers.
* DoneInclude security clauses in contracts with third parties.
* DoneMonitor supply chain risks and implement incident response plans.

#### **4. Incident Reporting and Response**

* DoneDevelop a formal incident response plan.
* DoneEnsure all employees are trained to identify and report incidents.
* DoneSet up mechanisms to detect and respond to cyber threats in real-time.
* DoneEstablish procedures to report significant incidents within the 24-hour timeframe required by NIS2.

#### **5. Legal and Compliance Requirements**

* DoneMap the NIS2 Directive requirements to your organization’s operations.
* DoneEnsure compliance with GDPR where applicable.
* DoneRegularly review and update policies to align with evolving regulations.
* DoneDocument all cybersecurity measures and compliance efforts.

#### **6. Training and Awareness**

* DoneProvide regular cybersecurity training for all employees.
* DoneConduct phishing and social engineering awareness campaigns.
* DoneEnsure stakeholders understand their responsibilities under NIS2.

#### **7. Continuous Improvement**

* DoneMonitor the cybersecurity landscape for new threats and vulnerabilities.
* DoneEstablish a continuous feedback loop for security measures.
* DoneParticipate in industry forums to stay updated on best practices.

###

### **Final Steps**

* DonePerform a gap analysis to identify areas of non-compliance.
* DoneConsult with legal and cybersecurity experts for guidance.
* DoneSchedule regular reviews to maintain NIS2 compliance.

### **Need More Guidance?**

**Visit the Heimdal blog for detailed insights and solutions to meet NIS2 requirements!**

**Download this checklist as a PDF for easy reference.**