NIS2 Compliance Checklist

This checklist provides a high-level overview of key actions required for NIS2 compliance. It should be used in conjunction with the full text of the NIS2 Directive and tailored to your organization's specific circumstances.

Phase 1: Assessment & Planning

□ Determine Applicability:

- Identify if your organization falls under NIS2 (Essential or Important entity).
- Determine which parts of your organization are affected.

□ Leadership & Governance:

- Assign responsibility for NIS2 compliance to a specific individual or team.
- Ensure management bodies understand their responsibilities and liabilities.
- Develop a cybersecurity training program for management.

□ Gap Analysis:

- Conduct a thorough assessment of current cybersecurity measures against NIS2 requirements.
- Identify gaps and areas for improvement in risk management, reporting, and business continuity.

□ Risk Assessment:

- Develop or update a comprehensive cybersecurity risk assessment process.
- Identify and prioritize cybersecurity risks based on their likelihood and potential impact.

□ Plan Development:

- Create a detailed NIS2 compliance plan with timelines and assigned responsibilities.
- Develop or update cybersecurity policies and procedures to align with NIS2.

Phase 2: Implementation

□ Risk Management Measures:

- Implement the 10 minimum baseline security measures (outlined in the whitepaper).
- Establish an incident handling plan and response process.
- Develop policies for vulnerability handling and disclosure.
- Implement access control measures and data protection policies.
- Implement cryptographic solutions, including encryption where appropriate.

□ Supply Chain Security:

- Assess the cybersecurity posture of direct suppliers.
- Incorporate NIS2 requirements into supplier contracts.

□ Business Continuity:

- Develop or update a business continuity plan for major cyber incidents.
- Establish backup and disaster recovery procedures.
- Form a crisis response team and define roles and responsibilities.

□ Reporting Obligations:

- Establish procedures for reporting significant incidents within the required timeframes (24-hour early warning, 72-hour detailed report, one-month final report).
- Designate a point of contact for communication with relevant authorities.

□ Training & Awareness:

- Provide cybersecurity training to all employees, including specific training for those with access to sensitive data.
- Conduct regular awareness campaigns to promote a culture of cybersecurity.

Phase 3: Monitoring & Improvement

□ Auditing & Assessment:

- Conduct regular internal audits to assess the effectiveness of security measures.
- Engage external auditors for independent verification of compliance.

□ Continuous Monitoring:

- Implement systems for ongoing monitoring of network and information systems.
- Regularly review and update risk assessments and security measures.

□ Incident Review:

- Conduct post-incident reviews to identify lessons learned and improve incident response procedures.

COPIA