Kiteworks

BEST PRACTICES

NIS2 Compliance Checklist

This NIS2 compliance checklist provides a step-by-step best practices guide to help organisations streamline their NIS2 compliance journey and position themselves for continued compliance. By following these best practices, organisations can enhance their security posture, fulfill their legal obligations, and contribute to a more secure digital environment.

- **1. Conduct Regular Risk Assessments:** Systematically identify, analyse, and evaluate cybersecurity risks to prioritise security efforts and allocate resources effectively, addressing the core NIS2 requirement of risk management.
- **2. Implement a Comprehensive Incident Response Plan:** Develop and maintain a detailed plan for detecting, responding to, and recovering from cybersecurity incidents. This ensures a quick and effective response to incidents, minimising impact and meeting NIS2's incident handling requirements.
- **3. Establish Strong Access Controls:** Implement robust authentication methods and least privilege principles to reduce the risk of unauthorised access and data breaches. This addresses NIS2's focus on network and information system security.
- **4. Conduct Regular Security Audits and Penetration Testing:** Perform periodic assessments of security controls and simulate cyberattacks to identify vulnerabilities and test the effectiveness of security measures, supporting continuous improvement as required by NIS2.
- **5. Implement Supply Chain Risk Management:** Assess and manage cybersecurity risks associated with suppliers and service providers. This addresses NIS2's emphasis on supply chain security, ensuring comprehensive risk management.
- **6. Provide Ongoing Cybersecurity Training:** Regularly educate employees on cybersecurity best practices and emerging threats to enhance your organisation's overall security posture. Security awareness training that addresses the human factor in cyber risk mitigation supports NIS2's requirement for organisational measures.

- **7. Establish a Vulnerability Management Program:** Systematically identify, assess, and remediate software and system vulnerabilities. Proactively addressing potential security weaknesses aligns with NIS2's risk management requirements.

- **8. Implement Data Protection and Privacy Measures:** Adopt strong data encryption, classification, and handling practices to protect sensitive information to support compliance with both NIS2 and other regulations like GDPR.

- **9. Develop and Maintain Asset Inventory:** Create and regularly update a comprehensive inventory of all IT assets and systems. This provides visibility into your organisation's attack surface, supporting effective risk management as required by NIS2.

- **10. Establish Metrics and Reporting Mechanisms:** Define key performance indicators (KPIs) for cybersecurity and implement regular reporting processes to enable continuous monitoring of compliance efforts. This also provides your organisation the necessary information for management oversight and potential incident reporting to authorities, as required by NIS2.