





NIS2 Compliance Best Practices Checklist



NIS2 compliance promotes a more uniform level of cybersecurity within the EU, protecting organisations, citizens, and the economy. Follow these NIS2 compliance best practices to enhance your security posture, fulfill your 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.
-  **2. Implement a Comprehensive Incident Response Plan:** Develop and maintain a detailed incident response plan for detecting, responding to, and recovering from cybersecurity incidents, ensuring a quick and effective response.
-  **3. Establish Strong Access Controls:** Implement robust authentication methods and least privilege principles. Strong access controls reduce the risk of unauthorised access and data breaches.
-  **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.
-  **5. Implement Supply Chain Risk Management:** Assess and manage cybersecurity risks associated with suppliers and service providers. Supply chain risk management ensures a more comprehensive risk management program.
-  **6. Establish a Vulnerability Management Program:** Systematically identify, assess, and remediate software and system vulnerabilities.
-  **7. Implement Data Protection and Privacy Measures:** Adopt strong data encryption, classification, and handling practices to protect sensitive information.
-  **8. Establish Metrics and Reporting Mechanisms:** Define key performance indicators (KPIs) for cybersecurity and implement regular reporting processes to enable continuous monitoring of compliance efforts.

