










NIS2 Compliance Best Practices Checklist for UK Businesses

The following best practices will help UK businesses adhere to NIS2 compliance requirements but also bolster their cybersecurity program to defend against cyberattacks and data breaches.

-  **1. Conduct a Comprehensive Risk Assessment:** Identify potential threats and vulnerabilities in your network and information systems. Evaluate the likelihood and impact of these risks to prioritise mitigation efforts.
-  **2. Implement Strong Access Controls:** Implement multi-factor authentication and role-based access controls (RBAC) to ensure that only authorised personnel have access to critical systems and data.
-  **3. Ensure Continuous Monitoring and Detection:** Implement advanced monitoring tools and techniques, such as intrusion detection systems and security information and event management solutions, to identify and respond to threats in real-time.
-  **4. Provide Regular Employee Training:** Conduct regular training sessions to educate employees about cybersecurity best practices, such as recognising phishing attempts and secure handling of sensitive data.
-  **5. Establish Clear Communication Channels:** Establish communication protocols for reporting incidents within your organisation and to relevant authorities as required by the NIS2 Directive.
-  **6. Collaborate with External Experts:** Consider consulting with specialists to assess your security posture, identify gaps, and recommend improvements.
-  **7. Invest in Advanced Cybersecurity Technologies:** Deploy solutions like next-generation firewalls, endpoint detection and response tools, and to safeguard your network and data.
-  **8. Secure the Supply Chain:** Conduct thorough assessments of your suppliers and third-party vendors to ensure they adhere to robust cybersecurity practices. Develop and implement policies and procedures to mitigate risks associated with third-party relationships.
-  **9. Integrate Threat Intelligence:** Utilise threat intelligence feeds and platforms to gather real-time information on potential risks. Integrate this intelligence into your monitoring and response efforts to proactively address threats.