Your NIS2 compliance checklist:

7 steps to prepare

The European Union's upcoming NIS2 Directive introduces new obligations on businesses to strengthen cybersecurity, audit regularly and report incidents swiftly. Compliance is mandatory for organisations providing essential services – but also vital for those competing to be their suppliers. Get your business NIS2-ready with these key actions.

1 Identify your cybersecurity risks

Vulnerabilities can hide throughout your network, systems and assets, leaving you exposed to risk. For example, unmanaged passwords or misconfigured or inactive accounts could be susceptible to credential theft. Conduct a comprehensive security evaluation to help pinpoint issues, assess their impact, and start taking steps to mitigate them.

Key action

Conduct a business-wide risk assessment and formulate a plan to reduce vulnerabilities.

2 Tighten access control

Blocking unauthorised access to systems and user accounts is crucial to preventing data breaches. Enforce strong access control with a robust Identity platform that centralises user management and allows you to define granular authorisation policies, ensuring only authorised individuals can access specific resources or perform certain actions.

Key action

Implement strong Identity governance to enforce stricter access control.

3 Safeguard privileged access

Adversaries can exploit privileged accounts to orchestrate attacks, take down critical infrastructure, and disrupt essential services. Safeguard privileged access by limiting access to administrator-level accounts and regularly rotating administrative passwords.

Key action

Protect privileged accounts with best practices such as least privilege access.

4 Implement phishing-resistant MFA

With social engineering attacks on the rise, NIS2 requires organisations to implement phishing-resistant Multi-Factor Authentication (MFA). This provides an extra layer of security when authenticating employees, customers and contractors, without adding friction to their digital experience.

Key action

Deploy phishing-resistant MFA to strengthen authentication without adding friction.

5 Strengthen your ransomware defences

Costly and debilitating ransomware attacks are one of the primary drivers of NIS2. Introduce security solutions to proactively defend against them, such as endpoint privilege management to enforce the principle of least privilege, control applications, and augment next-generation antivirus and endpoint detection and response solutions.

Key action

Introduce security solutions to proactively defend against ransomware, such as endpoint privilege management.

6 Scrutinise your software supply chain

The software you use from third-party vendors could be infected with malicious code. Take a fresh look at your software supply chain and consider implementing a secrets management solution to securely store sensitive data, such as passwords, keys and tokens.

Key action

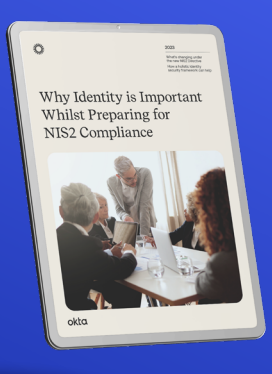
Consider implementing a secrets management solution to mitigate the risk of supply chain attacks.

7 Move to a Zero Trust strategy

Traditional perimeter-based security architectures aren't suited to today's borderless world of cloud services and hybrid workforces. Consider moving to a multi-layered Zero Trust approach, powered by strong Identity management, that enforces least privilege access, continuous authentication, and threat analytics.

Key action

Adopt an Identity-powered Zero Trust strategy that delivers the right access, to the right resources, at the right time.



Learn more about Identity and NIS2

Identity is the bedrock underpinning access to critical information. Through sound Identity management, organisations can control access, strengthen authentication and establish accountability with an easily accessible audit trail.

To learn more about how Identity helps ensure NIS2 compliance, read the whitepaper, **Why Identity is Important Whilst Preparing for NIS2 Compliance**

Download now