NIS2 Directive Checklist

A first step for your compliance journey, designed for organisations in the UK.

We suggest you check over the following aspects of your organisation's IT plan, the results of your assessment will give you a rough idea on how closely aligned you are to NIS2.

Asset management:

- ☐ Are your assets categorised based on their criticality and potential impact of a cyber incident?
- ☐ Do you have documented procedures for adding, removing, and updating assets?
- ☐ Are procedures in place for secure disposal of retired assets?

Risk management:

- ☐ Have you conducted a comprehensive risk assessment of your IT systems and data?
- ☐ Have you identified the potential threats, vulnerabilities, and potential impact of cyber incidents?
- ☐ Do you have documented risk mitigation strategies and controls in place?
- ☐ Do you regularly review and update your risk assessments?

Data and information security:

- ☐ Do you have data classification policies in place?
- ☐ Are sensitive data encrypted at rest and in transit?
- ☐ Are access controls implemented to restrict access to sensitive data based on the principle of least privilege?
- ☐ Do you have procedures for logging and monitoring data access?

Employee management:

- ☐ Do you have cyber security awareness training programs for all employees?
- ☐ Do you have policies on acceptable use of IT resources and password management?
- ☐ Do you have a process for investigating and reporting potential security incidents?

IT governance:

- ☐ Do you have a clearly defined cyber security governance structure?
- ☐ Are roles and responsibilities for cyber security clearly defined and documented?
- ☐ Do you have documented cyber security policies and procedures?
- ☐ Do you have a process for managing and documenting security incidents?

Supply chain management:

- ☐ Do you have security requirements in place for your suppliers and third-party vendors?
- ☐ Do you assess the cyber security risks associated with your supply chain?
- ☐ Do you have contracts with your suppliers that address cyber security responsibilities?

Incident reporting:

- ☐ Do you understand the NIS2 incident reporting requirements?
- ☐ Do you have a defined incident response plan?
- ☐ Do you have procedures for identifying, reporting, and responding to security incidents?
- ☐ Are your systems capable of collecting and preserving evidence of incidents?

Business continuity and crisis management:

- ☐ Do you have a business continuity plan (BCP) in place?
- ☐ Does your BCP address cyber incidents?
- ☐ Do you have crisis management procedures in place?
- ☐ Do you regularly test your BCP and crisis management plans?

Cyber security culture:

- ☐ Does your organisation promote a culture of cyber security awareness and responsibility?
- ☐ Do you encourage employees to report suspicious activity?
- ☐ Do you recognize and reward employees who exhibit good cyber security practices?

Monitoring and auditing:

- ☐ Do you have procedures for monitoring your IT systems and data for security threats?
- ☐ Do you regularly conduct internal audits to assess your cyber security posture?
- ☐ Do you keep records of your cyber security audits and assessments?

zenzero

Need assistance?

One of our cyber experts can walk you through everything you need to know.

GET IN TOUCH