

NIS2 Compliance Readiness Guide

**Strengthening Cybersecurity
and Resilience**

A practical readiness checklist
focused on cybersecurity,
compliance, and operational
resilience.

Why NIS2 readiness matters

A practical readiness checklist focused on cybersecurity governance, operational resilience, and regulatory compliance.

While NIS2 is an EU Directive, its requirements are based on widely recognised cybersecurity best practices and are increasingly used as a benchmark for resilience and risk management across industries globally.

This guide helps organisations assess whether they are prepared to prevent, detect, and respond to cyber incidents that could impact critical services and operations under the EU NIS2 Directive.

How to use this readiness guide

This guide is intended for organisations subject to the NIS2 Directive, as well as organisations seeking to align with NIS2 as a structured approach to cybersecurity, risk management, and operational resilience.

The assessment consists of a single one-page checklist covering key expectations related to governance, risk management, incident response, and supply chain security.

For each statement, select the option that best reflects your current situation:

- Yes - Implemented and operating effectively
- Not Sure - Don't know, partially implemented, or limited visibility
- No - Not implemented

Scoring

Each answer is scored as follows:

- Yes = 2 points
- Not Sure = 0 points
- No = 0 points

The checklist contains 10 questions with a maximum score of 20 points.

The score provides a high-level indication of NIS2 readiness and helps identify areas that may require further attention. It is intended as a practical self-assessment tool and not a formal compliance assessment.

1 Governance & leadership responsibility

a). Is responsibility for cybersecurity, operational resilience, and NIS2 compliance formally assigned and actively owned at management or board level?

Yes

Not Sure

No

b). Is leadership regularly informed about cyber risks that could impact critical services, business operations, or organisational resilience, and involved in approving related policies, risk management approaches, and mitigation measures?

Yes

Not Sure

No

2 Risk and asset management

a). Do you have a documented and up-to-date overview of IT systems, applications, infrastructure, and operational technologies, mapped to the critical services and operations they support?

Yes

Not Sure

No

b). Are systems and assets classified based on their impact on business continuity, service delivery, and operational risk, including risks related to downtime?

Yes

Not Sure

No

3 Vulnerability and patch management

a). Is there a documented vulnerability and patch management process that prioritises risks based on their potential impact on operations, security, and service availability?

Yes

Not Sure

No

b). Are technical constraints (e.g. system limitations, dependencies, or vendor restrictions) formally assessed, documented, and risk-accepted where remediation cannot be immediately applied?

Yes

Not Sure

No

4 Incident detection, response, and resilience

a). Do you have a documented and tested incident response plan with clearly defined roles, escalation paths, and procedures for handling cybersecurity incidents affecting critical systems and services?

Yes

Not Sure

No

b). Are backup, recovery, and continuity procedures in place and regularly tested for systems that are critical to business operations and service continuity?

Yes

Not Sure

No

5 Supply chain, monitoring, and compliance evidence

a). Do you have sufficient visibility and control over cybersecurity and availability risks introduced by critical suppliers, third parties, and externally managed systems?

Yes

Not Sure

No

b). Can you continuously monitor security-relevant events and demonstrate auditable evidence of cybersecurity controls, risk decisions, and NIS2-related compliance activities over time?

Yes

Not Sure

No

Interpreting your score

The checklist consists of 10 questions with a maximum score of 20 points. Each “Yes” answer indicates that a control is implemented and operating, while “No” and “Not Sure” highlight areas requiring attention.

Score interpretation

16–20 points – Strong baseline

Core NIS2 expectations are largely addressed. The focus should be on maintaining controls, strengthening documentation, and ensuring evidence is consistently available for management oversight and audits.

8–15 points – Partial readiness

Some key controls are in place, but important gaps remain. Management attention is required to formalise ownership, improve visibility across critical systems, and address areas that could impact operations, service delivery, or organisational resilience.

0–7 points – Early stage

Significant gaps exist in relation to NIS2 expectations. Immediate prioritisation is recommended to establish basic governance, risk management, and operational resilience measures to reduce exposure and support continuity of critical services.

The score should not be interpreted as a formal compliant/non-compliant judgement, but as a practical indication of readiness and prioritisation needs.

Important note

This readiness check reflects common expectations under the NIS2 Directive for organisations classified as essential or important entities.

Regulatory interpretation and enforcement may evolve, and professional or legal advice may be appropriate.

From readiness to action

At SecTeer, we help organisations secure and update their endpoints efficiently and proactively. With VulnDetect, we provide a complete endpoint security solution – from identifying and prioritising vulnerabilities with precise data to seamlessly patching both standard and third-party applications without disrupting end users, helping organisations move towards a more resilient and compliance-ready environment.

*This guide supports internal self-assessment and prioritisation only. It does not constitute an audit, certification, or formal compliance determination.