NIS2 Compliance Assessment Toolkit

A practical guide and self-assessment tools for organizations

The new cybersecurity regulations - the NIS2 Directive - introduce new obligations for many organizations. These requirements affect, in particular, medium and large enterprises that process data, provide digital services, or play an important role in the functioning of national or EU infrastructure. To help companies prepare effectively, we have developed three practical self-assessment tools that allow you to quickly and reliably evaluate your organization's level of compliance and operational readiness.

To help companies prepare effectively, we have developed three practical self-assessment tools that allow you to quickly and reliably evaluate your organization's level of compliance and operational readiness.

Purpose and scope of the toolkit

This toolkit has been created to help organizations independently assess their cybersecurity maturity and compliance with NIS2.

Each spreadsheet serves a specific purpose:

Full NIS2 Compliance Self-Assessment

A comprehensive tool covering all legal and organizational requirements. It helps organizations evaluate their preparedness for a full regulatory audit or inspection.

Initial NIS2 Compliance Audit

A simplified version designed to provide a quick overview — typically within one hour — of your company's current level of readiness. Perfect for executives and IT managers who want to identify key priorities before formal audits.

Operational Readiness Assessment (SOC & Incident Response)

A practical tool focused on the technical side of cybersecurity: how effectively your organization detects, responds to, and reports incidents in line with the law.

Legal and methodological foundations

The assessment sheets are based on:

Directive (EU) 2022/2555 - NIS2, on measures for a high common level of cybersecurity across the Union, including the draft amendment defining the obligations of essential and important entities, And internationally recognized standards and frameworks, including: **ENISA, ISO/IEC 27001. ISO/IEC 27005, ISO/IEC 27035, ISO 22301, NIST Cybersecurity Framework**, and CIS Controls v8.

Each sheet combines regulatory compliance with practical evaluation criteria, helping organizations align both management and technical aspects of cybersecurity.

Why these tools were created

Many organizations — especially in the SME sector — lack the time or internal resources to perform full cybersecurity audits. The purpose of these tools is to make the process accessible and clear by allowing organizations to:

Perform a quick and understandable assessment of their compliance with NIS2,

Identify key risk areas and set improvement priorities,

Facilitate communication between management and IT/security teams, And prepare for regulatory inspections or external audits in a structured way.

Key areas covered

The assessment covers all main areas verified during compliance audits and regulatory reviews:

Area	Scope of assessment
Governance and accountability	Whether the organization has appointed a person responsible for cybersecurity, implemented a security policy, and ensures management oversight of security matters.
Risk management and business continuity	Whether risk analysis processes are in place, continuity and recovery plans have been developed, and regular testing is performed.
Monitoring and threat detection	Whether the organization maintains continuous monitoring of IT systems, analyzes logs, and identifies unauthorized access attempts.
Incident response	Whether a formal incident response plan exists, is tested, and roles and responsibilities are clearly assigned.
Reporting and evidence management	Whether incidents are reported within required timeframes and all evidence is properly recorded and archived.
Auditing, training, and improvement	Whether internal audits, employee trainings, and post-incident reviews are regularly conducted.