SHIELDWORKZ

Comprehensive NIS2 Checklist with Evidence Required

October 2025

1. Introduction

This checklist is designed to be a practical tool for organizations to assess their preparedness and guide their compliance efforts. It covers the key obligations stemming from the directive, focusing on governance, risk management, security measures, and reporting.

Disclaimer: This checklist is intended as a comprehensive guide and should not be considered legal advice. Organizations must refer to the official text of the NIS2 Directive (Directive (EU) 2022/2555) and consult with legal and cybersecurity professionals to ensure full compliance based on their specific context, sector, and national transpositions.

Category/Domain	Requirement / Checklist Item	Status (e.g., Not Started, In Progress, Completed, N/A)	Notes / Evidence / Owner
1. Foundation & Scope	**1.1 Determine Applicability:** Confirm if the organization qualifies as an "Essential Entity" (EE) or "Important Entity" (IE) under the criteria in Annex I or II.		*Evidence: Sector analysis, size-cap evaluation, legal consultation.*
	1.2 Identify In-Scope Services: Clearly define and document all services provided by the organization that fall under the scope of NIS2.		*Evidence: Service catalogue, system architecture diagrams.*
	1.3 Register with the National Authority: Identify and complete the required registration process with the designated national competent authority.		*Owner: Compliance/Legal Team.*
2. Governance & Management Accountability (Article 20)	**2.1 Management Body Approval:** The management body (e.g., Board of Directors, C-suite) has formally approved the cybersecurity risk-management measures.		*Evidence: Board meeting minutes, signed policy documents.*
	2.2 Management Body Oversight: The management body actively oversees the implementation of the approved cybersecurity measures.		*Evidence: Regular reporting dashboards, dedicated agenda items in management meetings.*
	2.3 Mandatory Training: Members of the management body have undergone specific cybersecurity training to identify risks and assess risk-management practices.		*Evidence: Training certificates, course curriculum, attendance records.*
	2.4 Personal Liability: The management body understands its direct responsibility and potential liability for infringements of the risk management obligations.		*Evidence: Legal briefing documents, internal communications.*
3. Cybersecurity Risk Management Measures (Article 21)	**3.1 Risk Analysis & Security Policies:** An overarching policy on risk analysis and information system		*Evidence: Information Security Policy, Risk Assessment Methodology.*

Category/Domain	Requirement / Checklist Item	Status (e.g., Not Started, In Progress, Completed, N/A)	Notes / Evidence / Owner
	security has been established, approved, and implemented.		
	3.2 Incident Handling & Management: A formal incident handling process is in place, including procedures for detection, analysis, containment, eradication, and recovery.		*Evidence: Incident Response Plan (IRP), defined roles (e.g., CSIRT).*
	3.3 Business Continuity & Crisis Management: Business continuity and disaster recovery plans are established and tested. This includes backup management, disaster recovery, and crisis management protocols.		*Evidence: BCDR Plans, test results, crisis communication plan.*
	3.4 Supply Chain & Supplier Security: Security-related risks stemming from suppliers and service providers are identified and addressed. This includes risks from provider-to-provider relationships.		*Evidence: Third-party risk assessment process, security clauses in supplier contracts.*
	3.5 Security in System Lifecycle: Security measures are integrated into the acquisition, development, and maintenance of network and information systems (e.g., Secure SDLC).		*Evidence: Secure coding guidelines, vulnerability disclosure policy, change management process.*
	3.6 Effectiveness Assessment: Policies and procedures are in place to assess the effectiveness of the implemented cybersecurity risk-management measures.		*Evidence: Audit plans, penetration test reports, vulnerability assessment results.*
	3.7 Basic Cyber Hygiene & Training: Basic cyber hygiene practices are enforced (e.g., patching, configuration), and regular cybersecurity training is provided to all employees.		*Evidence: Patch management policy, security awareness training records, phishing simulation results.*
	3.8 Cryptography & Encryption: Policies and procedures regarding the use of cryptography and encryption (for data in transit and at rest) are defined and implemented where appropriate.		*Evidence: Cryptography policy, data classification scheme, public key infrastructure (PKI) documentation.*
	3.9 Human Resources Security: Procedures are in place for HR security, including pre-employment, in-employment, and post-employment phases.		*Evidence: Background check policy, termination checklist, role-based training plans.*
	3.10 Access Control & Asset Management: Strong access control		*Evidence: Access Control Policy, asset inventory,*

Category/Domain	Requirement / Checklist Item	Status (e.g., Not Started, In Progress, Completed, N/A)	Notes / Evidence / Owner
	policies (e.g., Principle of Least Privilege, Zero Trust principles) and a comprehensive asset management system are in place.		*privileged access management (PAM) solution.*
	3.11 Multi-Factor Authentication (MFA): MFA or continuous authentication solutions are deployed for all relevant systems, particularly for remote access, privileged users, and access to sensitive data.		*Evidence: MFA policy, technical configuration documents, logs from MFA systems.*
	3.12 Secure Communications: Secure voice, video, and text communication systems, as well as secure emergency communication systems within the entity, are established and maintained.		*Evidence: System architecture for secure comms, emergency contact lists.*
4. Reporting Obligations (Article 23)	**4.1 Significant Incident Definition:** Clear, internal criteria are defined for what constitutes a "significant incident" based on NIS2 guidelines (e.g., number of users affected, duration, geographical spread).		*Evidence: Incident Classification Matrix in the IRP.*
	4.2 24-Hour Early Warning: A process is established to submit an "early warning" to the national CSIRT or competent authority within 24 hours of becoming aware of a significant incident.		*Evidence: Documented procedure, designated reporting personnel, contact details for authorities.*
	4.3 72-Hour Incident Notification: A process is established to submit a detailed "incident notification" within 72 hours of becoming aware of the significant incident, updating the initial warning.		*Evidence: Template for incident notification, workflow diagram.*
	4.4 Intermediate / Progress Reports: Procedures are in place to provide intermediate reports upon request from the CSIRT or competent authority.		*Owner: Incident Response Team / Compliance.*
	4.5 Final Report (One Month): A process is in place to submit a comprehensive final report no later than one month after the submission of the incident notification.		*Evidence: Template for final report, root cause analysis procedure.*
5. Documentation & Compliance	**5.1 Maintain Documentation:** All policies, procedures, risk assessments, and implemented measures are thoroughly documented and readily available for audits.		*Evidence: Centralized repository of compliance documents (e.g., GRC tool, SharePoint).*

Category/Domain	Requirement / Checklist Item	Status (e.g., Not Started, In Progress, Completed, N/A)	Notes / Evidence / Owner
	5.2 Regular Audits: A schedule for regular internal and external audits is established to verify compliance with NIS2 requirements.		*Evidence: Audit schedule, past audit reports, corrective action plans.*
	5.3 Continuous Improvement: A process exists to review and update all security measures and policies based on lessons learned from incidents, new threats, and audit findings.		*Evidence: Management review meeting minutes, updated policy version history.*
	5.4 Information Sharing: The organization is prepared to participate in national and EU-level cybersecurity information-sharing arrangements when relevant.		*Evidence: Subscriptions to threat intel feeds, membership in an ISAC (Information Sharing and Analysis Center).*

Ready to secure your OT environment? Contact us today to discuss your NIS2 needs and take the definitive step towards robust industrial cybersecurity.