NIS2 Compliance Checklist 2026: A Comprehensive Guide to Audit-Readiness

FREE PDF

Prepared by :

Gart Solutions

Issued :

September 2026

gartsolutions.com

info@gartsolutions.com

Intro

NIS2 has moved from transposition into implementation and supervision. Organisations should now be prepared to demonstrate documented risk management, board oversight, tested incident reporting and supply-chain controls when requested by their competent authority.

The October 2024 transposition deadline has passed, but national implementation is not uniform.

On 9 July 2026, the European Commission referred Ireland, Spain, France and the Netherlands to the Court of Justice of the European Union over incomplete transposition. In Germany, the NIS2 Implementation Act took effect on 6 December 2025.

BSI registration through MELDUNG.BSI was due on 6 March 2026 and covers approximately 29,500 organisations across 18 sectors; the reported figure of approximately 18,500 missed registrations is an estimate from industry commentary, not an official enforcement statistic.

ENISA's NIS360 2026 assessment, published on 28 May 2026, reports improving maturity overall while identifying health, rail, maritime, ICT service management, space, public administration, and drinking and wastewater as sectors still in the risk zone. The practical standard is evidence: dated risk assessments, board oversight records, tested controls, current reporting contacts, and proof that incident procedures work against the legal clock.

Under NIS2 Article 23, incident response must support a 24-hour early warning, a 72-hour incident notification, and a final report within one month. This checklist helps you prepare the evidence an auditor or competent authority may request.

This isn't a checklist for getting ready before NIS2 arrives — it's a checklist for proving you're ready when the auditor calls.

The checklist is categorized into 8 categories and represents the updated areas in the NIS2 Directive:

1. Governance and Risk Management
2. Cybersecurity Policies and Procedures
3. Technical and Operational Measures
4. Security Technologies and Solutions
5. Technical Compliance and Certifications
6. Compliance with Legal and Industry Standards
7. Reporting and Communication
8. Human Resources and Training

To ensure that the NIS2 compliance framework aligns with your organization's strategic objectives and acceptable risk levels, it is crucial to review this **8 checklist points:**

1 . Governance and Risk Management

- [ ] Goals and risk appetite are defined.
- [ ] Roles and responsibilities for NIS2 compliance are assigned.
- [ ] Accountability in the event of non-compliance is specified.
- [ ] Cyber risks within the environment are identified and documented.
- [ ] Both internal and external factors affecting security are considered.
- [ ] Cybersecurity measures are regularly reviewed.
- [ ] Management-body accountability is documented and demonstrable: board approval, oversight records, and management cybersecurity-training evidence are retained.
- [ ] A risk assessment has been completed, dated, assigned an owner, and reviewed on a defined cycle.

2. Cybersecurity Policies and Procedures

- [ ] Security policies are documented, clearly understood, and assessed periodically.
- [ ] Formal incident response plans and handling are implemented, including a detailed ticketing system for incident detection, triage, and response to meet reporting obligations.
- [ ] Incident-response plans map to NIS2 Article 23: 24-hour early warning, 72-hour detailed notification, and final report within one month.
- [ ] Supply chain interactions are secured, and risks related to suppliers or service providers are mitigated, ensuring comprehensive security from end to end.
- [ ] Backup management and disaster recovery plans are established, aligning with agreed Recovery Time Objectives (RTOs) to ensure business continuity.

3. Technical and Operational Measures

- [ ] Basic cyber hygiene practices are assessed against CIS Controls v8.1 and NIST CSF 2.0, with evidence of implementation and review.
- [ ] Network and information systems are secured, with a focus on robust vulnerability handling and disclosure practices.
- [ ] Strong cryptography and encryption practices are used for sensitive data, including encrypting data at rest and in transit to protect sensitive information.
- [ ] Robust endpoint protection and network and information security measures are deployed to prevent unauthorized access and attacks.

4. Security Technologies and Solutions

- [ ] Comprehensive security solutions (including SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), and UEBA (User and Entity Behavior Analytics) tools) are employed. These solutions comply with standards such as Common Criteria EAL3+ and support GDPR, Schrems II, and CCPA regulations.
- [ ] SaaS solutions are used that comply with EU data residency regulations, such as GDPR for data protection.
- [ ] Cloud environments are secured against breaches and unauthorized access.
- [ ] Cloud and managed-service providers are assessed against the NIS2 technical implementing regulation, Commission Implementing Regulation (EU) 2024/2690, including its technical and methodological requirements for DNS providers, cloud providers, data centres, and managed service and managed security service providers.

5. Technical Compliance and Certifications

- [ ] Multi-factor authentication and secured communication systems are used for critical services, including voice, video, and text communications, especially for remote or privileged access.
- [ ] Relevant security frameworks are applied, and compliance with standards such as ISO 15408 for technology security and ISO/IEC 27001:2022 for information security management is ensured.

6. Compliance with Legal and Industry Standards

- [ ] The requirements of NIS2 are implemented, key differences from the original NIS Directive are noted.
- [ ] Cybersecurity strategies and frameworks to strengthen security posture and standards are implemented. In healthcare - HIPAA compliance, energy - NERC CIP standards, in finance - SOX compliance.
- [ ] NIST CSF 2.0, ISO/IEC 27001, and CIS Controls are implemented to strengthen security posture.
- [ ] Overlap with the Cyber Resilience Act (CRA) and DORA is mapped, with ownership, deadlines, authorities, and customer-notification duties reconciled across regimes.

7. Reporting and Communication

- [ ] To swiftly detect, analyze, and report significant incidents to relevant authorities (such as national CSIRTs) the infrastructure capabilities are developed.
- [ ] Governance processes and cybersecurity efforts are documented comprehensively.
- [ ] Benchmarks such as ISO/IEC 27002:2022 are used for standard compliance.
- [ ] The reporting process is automated as much as possible.
- [ ] Reporting workflows monitor and prepare for the EU's proposed move toward more consolidated incident reporting; a single-entry model is not yet fully operational.
- [ ] National CSIRT contacts, reporting portals, escalation owners, and access details are current and tested, including MELDUNG.BSI where relevant.

8. Human Resources and Training

- [ ] THR policies are implemented to control access based on roles, conduct regular security assessments, and enforce strict security training and awareness programs.
- [ ] Personnel is aware of cybersecurity best practices, data handling, and compliance obligations.
- [ ] Management-level cybersecurity training and expertise are documented, not only staff training; attendance, scope, and follow-up actions are retained.

Why Gart?

Gart Solutions is an IT Consulting partner, specialized in infrastructure setup, automatization, cloud migration, DevOps, Security, Compliance and more.

At Gart we have been helping our customers during the last 10 years to build digital products in the right way.

We work to solve your tech challenges on time and budget **to let you focus on what matters the most – growing your business.**

Book a Free NIS2 Readiness Assessment

Need help proving NIS2 compliance under active supervision? Regulators have moved from registration to audits, and management accountability is now a documented compliance expectation. Gart Solutions helps you close the gap before the auditor finds it.

gart.

Contributors

Fedir Kompaniiets

Co-Founder at Gart Solutions,
DevOps and Cloud Solutions Consultant

Roman Burdiuzha

Cloud Architect, Co-Founder and
CTO at Gart Solutions

gart.

Get in touch with us

gartsolutions.com

info@gartsolutions.com