NIS2 Compliance Checklist: A Comprehensive Guide to Audit

FREE PDF

Prepared by :

Gart Solutions

Issued :

July, 2024

gartsolutions.com

info@gartsolutions.com

Intro

NIS2 is an upgraded version of the original NIS Directive (NIS1), which was introduced by the European Commission in July 2016.

This new directive aims to significantly bolster cybersecurity measures across organizations within EU Member States.

By building upon the foundation of the original directive, NIS2 expands its reach to include additional sectors and organizations, addressing the evolving landscape of cyber threats.

NIS2 establishes a detailed framework that organizations must adhere to to enhance their cybersecurity and cyber resilience.

This framework is designed to protect critical information systems and personal data, while effectively responding to emerging cyber threats.

To help audit and improve your organization's cybersecurity practices, utilize this free NIS2 compliance checklist.

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 is involved in the approval and oversight process**.**

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.
- [ ] 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 and implemented, with regular cybersecurity training conducted to maintain high-security standards.
- [ ] 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.

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 27001 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 SP 800 series, ISO/IEC 27001, CIS Controls are implemented to strengthen security posture.

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.

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.

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.**

Need a help with NIS2 compliance assessment?

Gart Solutions can guide your organization through this journey. Address emerging cyber-attacks now, until the update, takes effect in October 2024.

Book a Free Consultation

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