NIS2 DIRECTIVE Compliance Checklist

A Comprehensive Guide for European Businesses

Deadline	October 17, 2024
Applies To	Essential and Important Entities in the EU
Penalties	Up to €10M or 2% of global turnover
Document Version	November 2025

Powered by Auth N Go - Passkey Authentication for NIS2 Compliance

---

Executive Summary

The NIS2 Directive (Directive (EU) 2022/2555) represents the European Union's updated framework for cybersecurity. It replaces the original NIS Directive and significantly expands the scope of entities required to implement robust cybersecurity measures. This checklist provides a comprehensive guide to achieving NIS2 compliance, with specific focus on authentication and access management requirements.

Key Changes from NIS1

- Expanded scope covering more sectors and entity types
- Stricter security requirements and risk management obligations
- Enhanced incident reporting requirements (24-72 hour timeline)
- Increased penalties for non-compliance
- Supply chain security obligations
- Mandatory use of multi-factor authentication
- **Personal liability for management –** Directors and managers can be held personally liable for compliance failures, including public naming and temporary bans from management positions

---

Why This Matters to Leadership

> ⚠️ **Critical: Personal Liability Under NIS2**
>
> NIS2 represents a fundamental shift in how cybersecurity compliance is enforced. For the first time, **directors and high-level managers are personally responsible** for ensuring compliance with the directive.
>
> **This is not something you can delegate to IT.**

What Personal Liability Means

Under NIS2, Member State authorities can hold organization managers personally liable if gross negligence is proven after a cyber incident. Consequences include:

- **Public identification** – Authorities can order that compliance violations be made public, identifying the natural and legal persons responsible
- **Management bans** – For essential entities, individuals can be temporarily banned from holding management positions in case of repeated violations
- **Personal financial sanctions** – Penalties can include fines up to 600% of salary in some member states
- **Reputational damage** – Public statements identifying responsible individuals damage personal and professional reputation

Management Responsibilities

The NIS2 Directive requires management bodies to:

1. **Approve** all cybersecurity risk management measures
2. **Oversee** their implementation
3. **Receive** specialized cybersecurity training
4. **Ensure** adequate resources are allocated
5. **Document** all security decisions and measures

Boards cannot delegate full responsibility to the IT department or compliance team. Members of the governing body may be held accountable for failures to implement and oversee required measures.

Article 21: Security Requirements

Article 21 of the NIS2 Directive outlines specific cybersecurity risk management measures that entities must implement. Below is a comprehensive checklist organized by requirement category.

1. Risk Management & Security Policies

- ☐ Conduct comprehensive risk assessments covering all information systems
- ☐ Develop and maintain incident handling procedures
- ☐ Implement business continuity plans (backup management and disaster recovery)
- ☐ Establish supply chain security measures
- ☐ Document security policies covering network and information systems
- ☐ Implement measures for assessing effectiveness of risk management

2. Authentication & Access Control

Auth N Go Solution: Our passkey-based authentication platform is specifically designed to meet and exceed these requirements. Passkeys provide hardware-backed, phishing-resistant authentication that eliminates password vulnerabilities.

Requirement	Status	Notes
Multi-factor authentication (MFA) for privileged access	Required	Passkeys provide cryptographic MFA
Strong authentication mechanisms	Required	Passkeys use public key cryptography
Access control policies and procedures	Required	Tenant’s application responsibility
Secure authentication protocols	Required	Passkeys use WebAuthn standard
Regular review of access rights	Required	Tenant’s application responsibility
Protection against credential theft	Required	Passkeys cannot be phished or stolen
Secure credential storage	Required	Hardware-backed credential storage

3. Asset Management

Note: Asset management is the tenant’s responsibility. Auth N Go focuses solely on authentication.

- ☐ Maintain inventory of all assets (hardware, software, data)
- ☐ Classify assets based on criticality and sensitivity
- ☐ Implement asset lifecycle management procedures
- ☐ Track and manage software licenses and versions
- ☐ Document data flows and processing activities

4. Cryptography & Data Protection

- ☐ Implement encryption for data at rest and in transit
- ☐ Use cryptographic controls for data confidentiality and integrity
- ☐ Maintain cryptographic key management procedures
- ☐ Ensure compliance with GDPR for personal data processing
- ☐ Implement data minimization principles
- ☐ Use strong cryptographic standards (e.g., TLS 1.3, AES-256)
  - *Auth N Go uses industry-standard encryption*

5. Network & Communications Security

- ☐ Segment network to isolate critical systems
- ☐ Implement firewalls and intrusion detection/prevention systems
- ☐ Secure network protocols and communications
- ☐ Monitor network traffic for anomalies
- ☐ Implement secure remote access solutions
- ☐ Regular vulnerability scanning and penetration testing

6. Incident Detection & Response

Reporting Timeline: Initial notification within 24 hours, full notification within 72 hours of incident awareness

- ☐ Establish incident response team with defined roles
- ☐ Implement 24/7 monitoring and detection capabilities
- ☐ Develop incident classification and escalation procedures
- ☐ Create incident response playbooks for common scenarios
- ☐ Implement automated alerting for security events
- ☐ Log all authentication events for incident analysis
  - *Auth N Go provides comprehensive audit trails*
- ☐ Establish communication procedures with authorities (CSIRTs)
- ☐ Document post-incident review process

7. Supply Chain Security

- ☐ Assess cybersecurity risks of suppliers and service providers
- ☐ Include security requirements in contracts with suppliers
- ☐ Monitor supplier compliance with security standards
- ☐ Establish procedures for supplier incident notification
- ☐ Verify security certifications of critical services
  - *Auth N Go: EU-hosted with GDPR compliance*
- ☐ Implement vendor risk management program

8. Security Training & Awareness

- ☐ Provide regular cybersecurity training to all employees
- ☐ Conduct specialized training for IT and security staff
- ☐ Implement phishing awareness campaigns
- ☐ Train users on proper authentication procedures
- ☐ Document training completion and maintain records
- ☐ Update training materials based on emerging threats

9. Governance & Management

Note: Organizational governance is the tenant’s responsibility. Auth N Go provides authentication infrastructure and compliance documentation.

⚠ **Management Liability Warning**

Under NIS2, directors and managers are personally responsible for ensuring compliance. Liability cannot be delegated to IT. Penalties for individuals include:

- Public identification as responsible for violations
- Temporary suspension from management positions
- Personal financial sanctions (up to 600% of salary in some member states)
- ☐ Designate management body responsible for cybersecurity
- ☐ Establish cybersecurity governance framework
- ☐ Conduct regular management reviews of security measures
- ☐ Allocate adequate resources for cybersecurity
- ☐ Maintain documentation of all security measures
- ☐ Implement continuous improvement processes
- ☐ **Ensure management receives mandatory cybersecurity training**
- ☐ **Document management approval of all security measures**

Implementation Roadmap

Achieving NIS2 compliance requires a structured approach. This roadmap provides a recommended timeline for implementing the required security measures.

Phase	Timeline	Key Activities	Priority
Assessment	2-4 weeks	Gap analysis, risk assessment, scope definition	Critical
Planning	2-4 weeks	Develop implementation plan, assign resources	Critical
Quick Wins	1-2 months	Implement MFA with Auth N Go, update policies	High
Core Security	3-6 months	Network security, encryption, monitoring	High
Governance	2-4 months	Training, documentation, procedures	Medium
Optimization	Ongoing	Continuous monitoring, improvement, audits	Medium

How Auth N Go Accelerates NIS2 Compliance

Auth N Go’s passkey-based authentication platform is specifically designed to address NIS2 authentication requirements and accelerate your compliance journey.

Requirement	Auth N Go Solution	Compliance Impact
Multi-Factor	Hardware-backed passkeys provide	Immediate compliance with

Requirement	Auth N Go Solution	Compliance Impact
Authentication	cryptographic MFA by default	Article 21(2)(e)
Phishing Resistance	Passkeys are bound to specific domains and cannot be phished	Eliminates #1 attack vector (81% of breaches)
Audit Trails	Comprehensive logging of all authentication events	Meets incident response and forensics requirements
EU Data Residency	100% EU-hosted infrastructure	GDPR compliant, supports data localization
Zero Password Vulnerabilities	No passwords means no password database to breach	Reduces attack surface significantly
Quick Implementation	5-minute integration with comprehensive SDKs	Accelerates compliance timeline

Getting Started with Auth N Go

1. **Sign Up:** Create your account at authngo.com
2. **Configure:** Set up your tenant and customize branding in minutes
3. **Integrate:** Use our SDKs for React, Angular, Vue, or vanilla JavaScript
4. **Deploy:** Go live with NIS2-compliant authentication
5. **Document:** Use Auth N Go's compliance reports for your NIS2 documentation

---

Additional Resources & References

Official NIS2 Documentation

- NIS2 Directive: Directive (EU) 2022/2555
- ENISA NIS2 Implementation Guide
- National transposition measures (check your country's cybersecurity authority)

Compliance Support

- Auth N Go Documentation: docs.authngo.com
- Technical Support: support@authngo.com
- Sales & Compliance Inquiries: sales@authngo.com
- Schedule a Demo: authngo.com/demo

AuthNGo Ltd.

Passkey Authentication for NIS2 Compliance

Ireland | EU-Hosted | GDPR Compliant

www.authngo.com

This document is provided for informational purposes only and does not constitute legal advice. Consult with qualified legal and cybersecurity professionals for compliance guidance specific to your organization.