NIS2 Readiness Checklist

Self-Assessment for EU Organizations

This checklist helps organizations assess their readiness for NIS2 Directive compliance. Use it to identify gaps and prioritize your security improvements.

NIS2 Deadline:	October 2024 (EU member state implementation)
Applies to:	Essential & important entities (50+ employees or €10M+ turnover)
Penalties:	Up to €10M or 2% global turnover for essential entities

Article 21: Cybersecurity Risk Management Measures

Article 21 of NIS2 defines 10 baseline measures that organizations must implement. Check your status for each area below.

Article 21(2)(a): Policies on risk analysis and information system security

- ■ Information security policy documented
- ■ Risk assessment process established
- ■ Risk register maintained
- ■ Regular policy reviews scheduled

Article 21(2)(b): Incident handling

- ■ Incident response plan documented
- ■ Incident classification criteria defined
- ■ Response team roles assigned
- ■ Communication procedures established

Article 21(2)(c): Business continuity and crisis management

- ■ Business continuity plan documented
- ■ Backup procedures implemented
- ■ Recovery time objectives defined
- ■ Crisis management procedures tested

Article 21(2)(d): Supply chain security

- ■ Supplier security requirements defined
- ■ Third-party risk assessments conducted
- ■ Software supply chain monitored
- ■ Vendor security reviews scheduled

Article 21(2)(e): Security in network and information systems acquisition

- ■ Security requirements in procurement
- ■ Secure development practices
- ■ Vulnerability handling procedures
- ■ Change management process

Article 21(2)(f): Policies and procedures for assessing effectiveness

- ■ Security metrics defined
- ■ Regular security assessments
- ■ Penetration testing program
- ■ Continuous monitoring in place

Article 21(2)(g): Basic cyber hygiene practices and training

- ■ Security awareness training program
- ■ Password policy implemented
- ■ Phishing awareness training
- ■ Regular training updates

Article 21(2)(h): Cryptography and encryption policies

- ■ Encryption policy documented
- ■ Data classification scheme
- ■ Key management procedures
- ■ Encryption of sensitive data

Article 21(2)(i): Human resources security and access control

- Access control policy documented
- Privileged access management
- User provisioning/deprovisioning
- Regular access reviews

Article 21(2)(j): Multi-factor authentication and secure communications

- MFA for privileged accounts
- MFA for remote access
- Secure communication channels
- Emergency access procedures

Gap Analysis & Prioritization

Use this section to identify your most critical gaps and plan remediation.

Priority	Gap Area	Current State	Target State	Due Date
Critical				
Critical				
High				
High				
Medium				
Medium				
Low				
Low				

Next Steps

1. Review gaps with your security team and management
2. Prioritize based on risk and effort required
3. Create an implementation roadmap with clear milestones
4. Assign ownership for each remediation area
5. Establish continuous monitoring to track progress

Automate Your NIS2 Compliance with VigilPrism

VigilPrism provides continuous security monitoring and compliance visibility across your entire environment. Deploy lightweight agents on Windows, Linux, and macOS to:

- Continuously scan systems against CIS Benchmarks and security best practices
- Map findings to NIS2 Article 21 requirements automatically
- Generate audit-ready reports in seconds, not days
- Track remediation from detection to resolution
- Maintain compliance evidence for regulatory reporting

Download the free Community Edition (3 agents forever free) at vigilprism.com