NIS2-self-assessment-checklist-2026

NIS2 Self-Assessment Checklist 2026

Essential Security Requirements for Operators of Critical Infrastructure

Branded for iso2700x.com

Document Information

- **Document Version:** 2026-Q1
- **Applicable Standard:** NIS2 Directive (EU 2022/2555)
- **Target Audience:** Critical Infrastructure Operators, Essential Service Providers
- **Completion Time:** 2-4 hours
- **Last Updated:** April 2026

Introduction

This checklist provides a comprehensive self-assessment framework for organizations subject to the NIS2 Directive. It aligns with the European Union's updated requirements for network and information system security across critical infrastructure sectors.

The NIS2 Directive expands the scope and raises security requirements for: - Energy (electricity, gas, oil, district heating) - Transport (air, rail, water, road) - Water and waste management - Health care - Digital infrastructure - Public administration - Financial services (critical functions) - Manufacturing of critical products - Space (satellite and ground segment operators)

Use this checklist to: 1. Identify existing security measures 2. Benchmark your organization's maturity 3. Plan remediation activities 4. Document compliance status 5. Support your NIS2 audit readiness

---

Section 1: Governance & Risk Management

Risk Assessment & Management

- ☐ Conduct annual network and information system risk assessments
- ☐ Document all identified risks with severity ratings (critical, high, medium, low)
- ☐ Establish risk tolerance thresholds approved by senior management
- ☐ Implement risk treatment plans with defined timelines
- ☐ Review and update risk assessments following significant changes
- ☐ Maintain a risk register accessible to security team and management
- ☐ Perform security impact assessments for new systems/services
- ☐ Document risk assessment methodology and criteria

Information Security Strategy & Policy

- ☐ Adopt a written information security policy endorsed by management
- ☐ Define security objectives aligned with organizational goals
- ☐ Establish clear roles and responsibilities for security governance
- ☐ Document security principles applicable to all stakeholders
- ☐ Include mandatory incident response procedures in policy
- ☐ Communicate security policy to all employees and contractors
- ☐ Review and update security policy annually or after major incidents
- ☐ Ensure board/executive oversight of information security

Governance Structure

- ☐ Designate a Chief Information Security Officer (CISO) or equivalent
- ☐ Establish information security steering committee
- ☐ Define escalation procedures for security incidents
- ☐ Document decision-making authority for security matters
- ☐ Ensure regular reporting to senior management (minimum quarterly)
- ☐ Include security in business continuity planning
- ☐ Align security governance with organizational structure

Section 2: Asset Management

Asset Inventory & Classification

- ☐ Maintain complete inventory of IT assets (hardware, software, data)
- ☐ Classify assets by criticality and sensitivity level
- ☐ Document owner and custodian for each asset
- ☐ Record asset locations and deployment details
- ☐ Update asset inventory when changes occur (quarterly minimum)
- ☐ Implement automated asset discovery tools where feasible
- ☐ Include third-party systems and cloud services in inventory

Data Management

- ☐ Identify and catalog all personal data processed
- ☐ Document data flows within and outside the organization
- ☐ Classify data by sensitivity (public, internal, confidential, restricted)
- ☐ Establish retention periods for each data type
- ☐ Implement secure disposal procedures
- ☐ Map data to systems and applications
- ☐ Document data residency and regulatory restrictions

Section 3: Access Control & Authentication

User Access Management

- ☐ Implement user access request and approval workflow
- ☐ Define role-based access control (RBAC) for all systems
- ☐ Review user access rights annually
- ☐ Immediately remove access upon employee departure
- ☐ Implement segregation of duties for critical functions
- ☐ Establish access for contractors with defined duration
- ☐ Document all system access decisions
- ☐ Maintain access audit logs for 90+ days

Authentication & Credentials

- ☐ Enforce multi-factor authentication (MFA) for all administrative accounts
- ☐ Require MFA for remote access (VPN, RDP, SSH)
- ☐ Implement strong password policy (minimum 12 characters, complexity)
- ☐ Enforce password expiration (maximum 90 days)
- ☐ Prohibit password reuse (last 5 passwords)
- ☐ Disable default credentials on all systems
- ☐ Use single sign-on (SSO) where technically feasible
- ☐ Implement privileged access management (PAM) for critical systems

Privilege Management

- ☐ Limit administrative access to necessary personnel only
- ☐ Implement just-in-time (JIT) privileged access elevation
- ☐ Log all privileged account activities
- ☐ Review privileged account usage monthly
- ☐ Establish separate administrative accounts (no shared accounts)
- ☐ Disable interactive administrative logins; require approval
- ☐ Implement automated privileged access reviews

Section 4: Cryptography & Data Protection

Encryption Standards

- ☐ Use encryption for all data in transit (TLS 1.2 minimum, 1.3 preferred)
- ☐ Implement encryption for sensitive data at rest
- ☐ Use NIST-approved or equivalent cryptographic algorithms
- ☐ Establish key management procedures (generation, storage, rotation)
- ☐ Rotate encryption keys annually or upon compromise
- ☐ Document cryptographic standards used across systems
- ☐ Implement hardware security modules (HSM) for critical keys
- ☐ Use certificates signed by trusted certificate authorities

Data Protection Measures

- ☐ Implement data masking for personal data in non-production environments
- ☐ Use tokenization for sensitive payment or health data
- ☐ Enable full-disk encryption on all mobile devices
- ☐ Encrypt backup data with secure, separately managed keys
- ☐ Implement secure data deletion procedures (cryptographic wiping)
- ☐ Restrict access to encryption keys on need-to-know basis

Section 5: Physical & Environmental Security

Facility Security

- ☐ Implement physical access controls (badges, biometrics) to sensitive areas
- ☐ Maintain security cameras with 90-day minimum retention
- ☐ Perform regular perimeter security inspections
- ☐ Establish visitor access procedures with registration
- ☐ Use environmental controls (climate, fire suppression)
- ☐ Implement intrusion detection/alarm systems
- ☐ Establish clear desk and clear screen policies
- ☐ Secure areas housing critical systems with restricted access

Device Security

- ☐ Install anti-theft devices on portable equipment
- ☐ Require screen locks on all computers/devices (5-min inactivity timeout)
- ☐ Use cable locks for equipment in shared spaces
- ☐ Implement full-disk encryption on all laptops/tablets
- ☐ Disable USB ports on sensitive workstations or manage via policy
- ☐ Remove unnecessary physical ports (COM, parallel)
- ☐ Securely dispose of decommissioned hardware (certified data destruction)

Section 6: Incident Management & Response

Incident Response Plan

- ☐ Document incident response procedures (detection, containment, eradication)
- ☐ Define incident severity classification (critical, high, medium, low)
- ☐ Establish incident response team with defined roles
- ☐ Provide incident response training annually
- ☐ Conduct incident response drills (tabletop exercises) semi-annually
- ☐ Maintain incident response contact list
- ☐ Define external escalation (law enforcement, regulators)
- ☐ Test incident response plan annually

Incident Detection & Logging

- ☐ Implement centralized security monitoring (SIEM or equivalent)
- ☐ Log authentication attempts (successes and failures)
- ☐ Log administrative and privileged actions
- ☐ Log data access for sensitive information
- ☐ Retain security logs for minimum 12 months
- ☐ Monitor for suspicious patterns (failed logins, unusual access)
- ☐ Alert on critical security events in real-time
- ☐ Implement tamper protection for logs

Breach Notification

- ☐ Establish timeline for incident reporting (NIS2 requires 72 hours)
- ☐ Designate point of contact for regulatory notification
- ☐ Implement breach notification procedures to affected individuals
- ☐ Document all incidents with timeline and impact assessment
- ☐ Prepare breach notification communication templates
- ☐ Know your competent authority contact information
- ☐ Maintain breach notification log for audit purposes

Section 7: Supply Chain Security

Third-Party Risk Management

- ☐ Conduct security assessments of critical suppliers
- ☐ Establish supplier security requirements in contracts
- ☐ Require security certifications (ISO 27001, SOC 2, etc.) where appropriate
- ☐ Maintain inventory of critical third-party dependencies
- ☐ Define escalation procedures for supplier security incidents
- ☐ Perform annual supplier security reviews
- ☐ Implement supplier incident notification requirements (timeline, content)

☐ Require right-to-audit clauses in critical supplier contracts

Software & Hardware Supply Chain

☐ Verify software/firmware authenticity and integrity
☐ Use trusted sources only for critical components
☐ Implement software bill of materials (SBOM) tracking
☐ Monitor for known vulnerabilities in dependencies
☐ Establish procedures for component and supply chain compromises
☐ Document software and firmware versions in use
☐ Implement secure update and patch management processes
☐ Maintain vendor contact information for security advisories

---

Section 8: Vulnerability & Patch Management

Vulnerability Assessment

☐ Conduct vulnerability assessments (quarterly minimum, more frequently for critical systems)
☐ Use automated vulnerability scanning tools
☐ Document vulnerabilities with severity ratings
☐ Prioritize remediation based on risk and criticality
☐ Establish timelines for vulnerability remediation
☐ Track remediation status and close-out
☐ Perform penetration testing annually
☐ Document and remediate findings from penetration tests

Patch Management

☐ Establish patch management policy with prioritization criteria
☐ Deploy critical patches within 30 days
☐ Deploy high-risk patches within 60 days
☐ Test patches in non-production environment before deployment
☐ Document all patching activities
☐ Implement automated patch deployment where feasible
☐ Monitor for patch availability from vendors
☐ Maintain inventory of systems that cannot be patched

Section 9: Security Operations & Monitoring

Continuous Monitoring

☐ Implement 24/7 security monitoring for critical systems
☐ Use intrusion detection/prevention systems (IDS/IPS)

☐ Monitor network traffic for anomalies
☐ Implement endpoint detection and response (EDR)
☐ Alert on unauthorized access attempts
☐ Monitor privileged account activities
☐ Review security alerts weekly at minimum
☐ Maintain audit trails for all security events

Change Management

☐ Implement formal change control process
☐ Require security review for all infrastructure changes
☐ Document all changes (what, who, when, why)
☐ Maintain rollback procedures for critical changes
☐ Test changes in non-production before deployment
☐ Implement approval workflow for security-critical changes
☐ Track change implementation and validation

Section 10: Supplier & Third-Party Management

Managed Services & Cloud Security

☐ Establish service level agreements (SLAs) with security requirements
☐ Define data protection requirements for cloud services
☐ Verify cloud provider security certifications
☐ Establish incident notification requirements (timeline, detail)
☐ Implement audit rights for critical cloud services
☐ Define data location and residency requirements
☐ Establish backup and disaster recovery requirements
☐ Maintain contracts with clear security clauses

Outsourced Operations

☐ Monitor outsourced security operations (if applicable)
☐ Establish service performance metrics
☐ Conduct quarterly reviews of outsourced services
☐ Implement escalation procedures
☐ Maintain audit trails for outsourced services
☐ Require security incident reporting within defined timelines

---

Section 11: Business Continuity & Disaster Recovery

Continuity Planning

☐ Develop business continuity plan (BCP) for critical functions

- ☐ Define recovery time objectives (RTO) and recovery point objectives (RPO)
- ☐ Identify single points of failure
- ☐ Establish backup systems for critical applications
- ☐ Implement geographic diversity for backups
- ☐ Document recovery procedures
- ☐ Test BCP annually with documented results
- ☐ Update BCP following significant changes

Disaster Recovery

- ☐ Implement regular backup procedures (daily minimum for critical data)
- ☐ Test backup restoration (monthly minimum)
- ☐ Maintain backup inventory and documentation
- ☐ Store backups off-site with secure access
- ☐ Encrypt all backups
- ☐ Verify backup integrity regularly
- ☐ Define backup retention periods per regulatory requirements
- ☐ Test disaster recovery procedures semi-annually

Section 12: Compliance & Audit

Regulatory Compliance

- ☐ Maintain register of applicable legal/regulatory requirements
- ☐ Document compliance status against NIS2 requirements
- ☐ Implement procedures for new regulatory requirements
- ☐ Maintain compliance documentation for audit
- ☐ Report compliance status to management quarterly
- ☐ Designate compliance responsibility
- ☐ Track regulatory changes in your sector

Internal Audit & Assessment

- ☐ Conduct annual internal security audits
- ☐ Document audit findings and recommendations
- ☐ Track remediation of audit findings
- ☐ Implement corrective actions with defined timelines
- ☐ Maintain audit working papers
- ☐ Review controls quarterly
- ☐ Perform self-assessments against NIS2 requirements

Section 13: Security Awareness & Training

Employee Training

- ☐ Provide mandatory security awareness training annually
- ☐ Include phishing awareness in training curriculum
- ☐ Provide role-specific security training (system admins, developers, etc.)
- ☐ Conduct security training for new hires during onboarding
- ☐ Maintain training records
- ☐ Test knowledge through phishing simulations (quarterly)
- ☐ Track training completion and address gaps
- ☐ Update training content annually

Security Culture

- ☐ Establish clear security expectations in job descriptions
- ☐ Include security performance in employee evaluations
- ☐ Recognize and reward security-conscious behavior
- ☐ Establish safe reporting channels for security concerns
- ☐ Communicate security incidents (lessons learned) to staff
- ☐ Foster open discussion of security issues

Scoring & Assessment

Completion Instructions

1. Review each section carefully
2. Check boxes that represent your current state
3. Calculate percentage by section
4. Identify gaps for remediation planning
5. Prioritize high-impact/high-risk gaps

Assessment Levels

Level 1 (Ad-hoc): <25% requirements met **Level 2 (Developing):** 25-50% requirements met **Level 3 (Defined):** 50-75% requirements met **Level 4 (Optimized):** >75% requirements met

---

Next Steps

1. **Identify Gaps:** Review unchecked items
2. **Prioritize:** Focus on critical infrastructure controls first
3. **Remediate:** Develop action plans for gaps
4. **Monitor:** Track progress on remediation
5. **Certify:** Consider ISO 27001 certification alongside NIS2 compliance

About iso2700x.com

iso2700x.com provides compliance consulting, training, and certification services for critical infrastructure operators, essential services, and organizations seeking to strengthen their information security posture.

Document Classification: Unclassified **Last Revised:** April 2026 **Next Review:** April 2027