bluegrid.io

SOC as a Service

NIS2 Compliance Checklist

bluegrid.io

NIS2 Compliance Checklist

General Compliance Requirements (Applicable to All Sectors)

1. Governance & Risk Management

- ☐ Assign cybersecurity responsibilities to senior management.
- ☐ Establish and document a cybersecurity governance framework.
- ☐ Develop and maintain a formal cybersecurity policy.
- ☐ Conduct regular risk assessments covering cyber threats, operational risks, and supply chain vulnerabilities.
- ☐ Ensure ongoing compliance with national cybersecurity regulations and industry best practices.

2. Network & System Security

- ☐ Implement network segmentation between IT and operational technology (OT) systems.
- ☐ Use firewalls, intrusion detection/prevention systems (IDS/IPS), and secure access controls.
- ☐ Deploy and regularly update endpoint security solutions (anti-malware, EDR).

- ☐ Enforce secure remote access using VPN and multi-factor authentication (MFA).
- ☐ Encrypt sensitive data at rest and in transit.

3. Identity & Access Management (IAM)

- ☐ Use role-based access control (RBAC) to limit access to critical systems.
- ☐ Implement MFA for all administrative and remote access accounts.
- ☐ Enforce privileged access management (PAM) for critical systems.
- ☐ Immediately revoke or adjust user access when employment roles change.

4. Incident Response & Reporting

- ☐ Develop and document a cybersecurity incident response plan (IRP).
- ☐ Establish a 24/7 monitoring system for real-time threat detection.
- ☐ Ensure initial incident notification within **24 hours**.
- ☐ Submit a full incident report within **72 hours**.
- ☐ Maintain ongoing collaboration with national cybersecurity agencies (CSIRTs).

5. Business Continuity & Disaster Recovery

- ☐ Implement and regularly test business continuity plans (BCP) for cyber-related disruptions.
- ☐ Develop a disaster recovery (DR) strategy, including rapid system restoration protocols.
- ☐ Maintain encrypted offline backups of critical data and system configurations.
- ☐ Conduct regular crisis simulation exercises (e.g., ransomware attack response drills).

6. Supply Chain Security

- ☐ Conduct cybersecurity risk assessments for all third-party vendors and service providers.
- ☐ Establish contractual cybersecurity obligations for vendors handling sensitive systems or data.
- ☐ Monitor and control third-party access to operational and IT systems.
- ☐ Regularly audit supply chain components for security vulnerabilities.

7. Physical & Environmental Security

- ☐ Secure physical access to IT and operational control centers.
- ☐ Protect against environmental threats such as power failures, fires, floods, or sabotage.
- ☐ Implement surveillance and access monitoring for sensitive infrastructure.

8. Training & Awareness

- [ ] Provide cybersecurity training to all employees handling critical systems.
- [ ] Conduct periodic phishing simulations and social engineering awareness training.
- [ ] Run cybersecurity response drills for employees and management.
- [ ] Continuously update training materials based on emerging cyber threats.

9. Compliance Management & Audit Preparedness

- [ ] Maintain detailed records of cybersecurity policies, incident reports, and risk assessments.
- [ ] Conduct regular internal audits aligned with ISO/IEC 27001 and other relevant standards.
- [ ] Ensure readiness for external regulatory audits and compliance checks.

---

bluegrid.io

Sector-Specific Compliance Requirements

Manufacturing

- ☐ Implement robust security for Industrial Control Systems (ICS) and SCADA environments.
- ☐ Secure automated production line systems and robotics from cyber threats.
- ☐ Protect Product Lifecycle Management (PLM) software and intellectual property.
- ☐ Ensure secure remote access for maintenance vendors and suppliers.

Energy

- ☐ Enforce strict security controls for electricity, oil, and gas infrastructures.
- ☐ Secure remote monitoring and control of energy distribution networks.
- ☐ Implement real-time anomaly detection for grid security.
- ☐ Align with EU Resilience of Critical Entities Directive (CER Directive).

Transport

- ☐ Secure signaling systems, air traffic control, and rail/road transport IT infrastructure.
- ☐ Implement cybersecurity measures for GPS tracking and fleet management.
- ☐ Protect online ticketing and payment processing platforms.
- ☐ Ensure maritime and aviation cybersecurity compliance.

Healthcare

- ☐ Secure Electronic Health Records (EHR) and patient data against breaches.
- ☐ Implement security controls for medical IoT devices and imaging systems.
- ☐ Enforce strong authentication for hospital IT and remote patient monitoring.
- ☐ Protect telemedicine and cloud-based healthcare platforms.

Digital Providers

- ☐ Secure cloud computing platforms, data centers, and content delivery networks (CDNs).
- ☐ Protect online marketplaces, search engines, and social media platforms from cyber threats.
- ☐ Ensure compliance with GDPR and EU eIDAS regulations for trust service providers.
- ☐ Mitigate risks related to DDoS attacks and API security vulnerabilities.

Drinking Water & Wastewater Management

- ☐ Secure SCADA systems controlling water treatment and distribution.
- ☐ Protect real-time monitoring systems for water quality and supply control.
- ☐ Implement cybersecurity protections for wastewater management plants.
- ☐ Ensure backup redundancy for critical infrastructure continuity.

Postal & Courier Services

- ☐ Secure parcel tracking systems and delivery logistics platforms.
- ☐ Implement strong authentication for customer accounts and postal staff.
- ☐ Protect customer data and address fraud prevention measures.
- ☐ Secure payment processing for online postal services.

Waste Management

- ☐ Protect ICS/SCADA systems controlling automated waste sorting and recycling.
- ☐ Implement cybersecurity protections for fleet and logistics tracking software.
- ☐ Secure environmental data monitoring and regulatory reporting systems.
- ☐ Ensure continuity of critical waste management operations in cyber incidents.

Banking & Finance

- ☐ Enforce strong authentication and fraud prevention for online banking.
- ☐ Secure financial market infrastructure (clearinghouses, trading platforms).
- ☐ Implement end-to-end encryption for transactions and customer data.
- ☐ Align with financial sector cybersecurity regulations (e.g., PSD2, GDPR).

Space

- ☐ Secure ground-to-space communication and satellite command control systems.
- ☐ Protect satellite telemetry, tracking, and command (TT&C) networks.
- ☐ Ensure cybersecurity for mission-critical space exploration and research systems.
- ☐ Implement real-time threat monitoring for satellite network infrastructure.

Research Organizations

- ☐ Protect intellectual property and sensitive research data against cyber espionage.

- ☐ Secure high-performance computing (HPC) clusters and research collaboration platforms.
- ☐ Implement strict access controls for sensitive laboratory and academic research systems.
- ☐ Align cybersecurity policies with GDPR and EU research data security standards.

References & Legal Framework

- **Directive (EU) 2022/2555 (NIS2 Directive)** – Articles 21 (Risk Management) & 23 (Incident Reporting)
- **ISO/IEC 27001** – Information Security Management Systems
- **ISO 22301** – Business Continuity Management
- **IEC 62443** – Industrial Control Systems Cybersecurity
- **ENISA Cybersecurity Guidelines** (sector-specific)
- **Resilience of Critical Entities Directive (CER Directive)** – Security measures for critical infrastructure
- **GDPR (EU 2016/679)** – Data protection requirements (where applicable)

This checklist provides a structured framework for organizations to achieve NIS2 compliance, covering both general and sector-specific cybersecurity requirements. Regular assessments and proactive security improvements will ensure a strong and resilient cybersecurity posture.

Self-Assessment System

To perform the self-assessment:

1. **Evaluate each requirement** listed in the compliance checklist.
2. Assign one of the three statuses (✅, ⚠️, or ❌) to each item based on your organization's current state.
3. Multiply the total number of checklist items by the maximum score (5 points per item) to determine the highest possible score.
4. Sum up the points earned based on your assessment:
    - **Fully compliant (✅) = 5 points**
    - **Partially compliant (⚠️) = 2 points**
    - **Non-compliant (❌) = 0 points**
5. Calculate your percentage compliance using this formula:
   (Fully compliant × **5 points**) + (⚠️ Partially compliant × **2 points**) + (❌ Non-compliant × **0 points**) = **Points Scored**

Total possible points:
(**Total number of checklist items** × **5 points** per item)

Result = ({**Points Scored**}/{**Total possible points**}) × 100

Result interpretation:

- **90-100%:** Excellent compliance.
- **75-89%:** Good – Minor improvements required.
- **50-74%:** Moderate – Immediate attention required.
- **<50%:** Poor – Critical improvements urgently needed.

Become NIS2 Compliant!

Book a FREE consultation call with our cybersecurity team!

bluegrid.io

Congrats!
You took the first step towards NIS2 compliance. We are here if you need a support in the process.

Book a Call

or

write to us: sales@bluegrid.io