NIS2 Technical Controls Assessment

Standards: NIS2 Directive 2022

Status: in-progress

Score: 100%

Assessor: Sarah Martinez

Started: 2024-03-10

Generated: 2025-07-10

Assessment Summary

Metric	Value
Total Requirements	12
Fulfilled	12
Partially Fulfilled	0
Not Fulfilled	0
Not Applicable	0
Compliance Score	100%

Detailed Requirements Results

A1 - Risk management measures

Status: FULFILLED

Implement appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems.

Notes:
NIS2 Directive Article 21 requirement

A2 - Incident handling

Status: FULFILLED

Implement measures to prevent and minimise the impact of incidents affecting the security of the network and information systems.

Notes:
NIS2 Directive Article 23 requirement - Focus on network and information systems specifically. Emphasize prevention and impact minimization. Ensure coordination with business continuity plans and consider cross-border incident implications for essential services.

Evidence:
Required Evidence Examples:
• Network Incident Response Procedures - Specialized procedures for network-specific incidents including DDoS attacks, network intrusions, and infrastructure failures
• Incident Prevention Measures - Proactive security controls including network monitoring, intrusion detection systems, and threat intelligence integration
• Impact Minimization Protocols - Procedures for rapid containment and isolation of network incidents to prevent spread and minimize business disruption
• Network Segmentation Plans - Technical documentation showing network architecture designed to contain and limit incident impact
• Incident Escalation Matrix - Clear escalation procedures for different types of network and information system incidents
• Recovery Time Objectives (RTO) - Defined target recovery times for critical network and information systems based on business impact
• Incident Communication Procedures - Internal and external communication protocols specific to network and information system incidents
• Business Continuity Integration - Coordination between incident response and business continuity procedures for network services
• Vendor Coordination Procedures - Protocols for engaging third-party vendors during network and information system incidents
• Incident Metrics and Reporting - KPIs for measuring incident response effectiveness and compliance with NIS2 requirements

A3 - Business continuity

Status: FULFILLED

Implement policies and procedures to ensure the continuity of critical services in case of incidents.

Notes:
NIS2 Directive requirement

A4 - Supply chain security

Status: FULFILLED

Address security risks in the supply chain, including with regard to the security-related aspects of the relationships between each entity and its direct suppliers or service providers.

Notes:
NIS2 Directive Article 21 requirement

A5 - Security in network and information systems acquisition

Status: FULFILLED

Evaluate and take into account security risks associated with the acquisition, development and maintenance of network and information systems.

Notes:
NIS2 Directive requirement

B1 - Incident notification

Status: FULFILLED

Notify the competent authority or the CSIRT of any incident having a significant impact on the provision of their services within 24 hours of becoming aware of the incident.

Notes:
NIS2 Directive Article 23 requirement - Critical 24-hour notification deadline for significant incidents. Requires clear impact assessment criteria and coordination with multiple authorities. Consider cross-border implications for essential services and ensure regular testing of notification procedures.

Evidence:
Required Evidence Examples:
• Significant Impact Assessment Framework - Criteria for determining when incidents have significant impact on service provision requiring notification
• Authority Contact Database - Current contact information for competent authorities and CSIRTs in all relevant jurisdictions
• 24-Hour Notification Procedures - Step-by-step process ensuring regulatory notification within 24-hour deadline
• Incident Notification Templates - Pre-approved notification formats meeting NIS2 reporting requirements
• Escalation Decision Tree - Clear criteria for determining when incidents require authority notification
• Cross-Border Notification Procedures - Process for notifying authorities when incidents affect services across multiple EU member states
• CSIRT Collaboration Protocols - Procedures for coordinating with national and EU-level Computer Security Incident Response Teams
• Service Impact Assessment Tools - Methods for quickly assessing and documenting impact on essential or important services
• Notification Tracking System - Records of all authority notifications including timestamps and follow-up communications
• Legal Review Procedures - Process for engaging legal counsel to review notification requirements and draft communications

B2 - Vulnerability handling and disclosure

Status: FULFILLED

Implement policies and procedures regarding coordinated vulnerability disclosure for previously unknown vulnerabilities.

Notes:
NIS2 Directive Article 22 requirement

B3 - Use of cryptography and encryption

Status: FULFILLED

Implement state-of-the-art cryptography and encryption where appropriate.

Notes:
NIS2 Directive requirement

B4 - Multi-factor authentication

Status: FULFILLED

Implement multi-factor authentication or continuous authentication solutions for systems processing sensitive data or providing critical functions.

Notes:
NIS2 Directive requirement

C1 - Basic cyber hygiene practices

Status: FULFILLED

Implement basic cyber hygiene practices and cybersecurity training for staff.

Notes:
NIS2 Directive requirement

... and 2 more requirements