Network and Information Security Directive (NIS2)

Compliance checklist

Are your OT operations NIS2 compliant?

Regardless of whether your facilities were compliant with the original NIS directive of 2016, it's important to take note of NIS2, as it introduces several significant changes.

- The directive now applies to new sectors not covered by the original NIS directive, such as water, waste management and critical manufacturing, among others
- Entities subject to NIS2 must conduct a risk analysis of their cybersecurity posture and establish documented security processes and incident-handling procedures
- The supply chain is now included, requiring affected entities to assess their supply chain's cybersecurity and implement suitable risk-management measures
- Rules for incident notification have become significantly stricter and entities are required to notify authorities of any suspected malicious act affecting their IT or OT networks within 24 hours

To begin your NIS2 compliance journey, follow these crucial steps:

1. Governance and risk management

✓ Set organisational goals and risk appetite to ensure the NIS2 compliance framework aligns with strategic aims and acceptable risk levels.

✓ Define specific roles and responsibilities for NIS2 tasks, designating accountability for non-compliance.

✓ Identify and document cyber risks in your environment, considering internal and external factors affecting security.

✓ Regularly review cybersecurity measures, ensuring management's active approval and oversight.

2. Cybersecurity policies and procedures

✓ Make sure security policies are well-documented, clearly communicated and periodically reviewed.

✓ Establish formal incident response plans, including a detailed ticketing system for detecting, triaging, and responding to incidents to fulfill reporting requirements.

✓ Protect supply chain interactions and address risks associated with suppliers or service providers, ensuring comprehensive security from start to finish.

✓ Create backup management and disaster recovery plans that meet agreed Recovery Time Objectives (RTOs) to ensure business continuity.

✓ Use the audit results to perform a gap analysis, pinpointing areas where your IT and OT networks need reinforcement and upgrades for NIS2 compliance.

3. Technical and operational measures

✓ Evaluate and establish fundamental cyber hygiene measures and regularly provide cybersecurity training to uphold stringent security protocols.

✓ Ensure the security of your network and information systems by prioritising comprehensive vulnerability management and disclosure procedures.

✓ Implement strong cryptographic methods and encryption standards to safeguard sensitive data, including encrypting data both at rest and in transit.

✓ Install advanced endpoint protection and enforce rigorous network and information security strategies to avert unauthorised access and cyber threats.

✓ During operational and optimisation stages, it is crucial that maintenance and incident recovery in a distributed industrial plant and machinery be executed promptly to prevent operational and service disruptions.

4. Security technologies and solutions

✓ Employ comprehensive security solutions

✓ Make sure they meet regulatory standards

✓ Use solutions that adhere to EU data residency laws

✓ Secure cloud environments against breaches and unauthorised access

5. Technical compliance and certifications

- ✓ Implement multi-factor authentication and secure communication systems for essential services, covering voice, video, and text communications, particularly for remote or privileged access.
- ✓ Adopt applicable security frameworks and guarantee compliance with standards s for technology security and for information security management.
- ✓ Leverage established cybersecurity frameworks like NIST SP 800-82 or IEC 62443, alongside appropriate expertise, to develop a bespoke NIS2 compliance framework.
- ✓ Unauthorised access to machines can result in downtime. Ensure that only authorised and adequately trained personnel always have access. Robust access control safeguards system integrity.

6. Compliance with legal, industry standards

- ✓ Understand and apply the NIS2 requirements, taking note of key differences from the original NIS Directive.
- ✓ Ensure your cybersecurity strategies align with the specific needs of critical infrastructure sectors
- ✓ Adopt recognised frameworks to enhance security practices and standards.
- ✓ Implement robust security measures to achieve transparency and create a security roadmap. Collaborate with expert engineers, process specialists, and consultants to put your framework into practice and ensure your organisation complies with the standards.
- ✓ Establish a program encompassing procedures for monitoring, risk and crisis management, incident response, optimisation and continuous improvement to maintain compliance and protect your organisation against threats.

7. Reporting and communication

- ✓ Develop capabilities to promptly detect, analyse and report significant incidents to appropriate authorities and notify impacted stakeholders, while adhering to prescribed timelines and content requirements.
- ✓ Thoroughly document governance processes and cybersecurity efforts. Employ standards for compliance and automate reporting procedures wherever feasible.
- ✓ Unauthorised access to machines can result in downtime. Ensure access is always restricted to authorised and trained personnel, safeguarding system integrity through robust access control mechanisms.
- ✓ New vulnerabilities are reported daily across numerous systems. Attackers can exploit vulnerabilities if proper mitigation measures are not implemented. Promptly identifying new vulnerabilities and minimising time required to apply patches are crucial. Vulnerability scanners can assess networks for potential entry points aimed at compromising systems and data.

8. Human resources and training

- ✓ Enforce HR policies that stringently manage access depending on roles, carry out frequent security evaluations, and mandate robust training and awareness initiatives on security.
- ✓ Equip your staff with thorough training on cybersecurity best practices, data management, and compliance responsibilities.
- ✓ Develop training and awareness programs to educate and enable employees at all levels to identify and counter cyber threats.
- ✓ Establish a culture focused on cybersecurity; this is crucial for maintaining long-term compliance.

Why Wood ...

Automation and Systems Integration

Risk assessment

Wood will assess security risks on all OT assets including reviews of current risk management, detection and response procedures and capabilities.

Close the gap

Following an assessment of your operations, Wood will examine your current cybersecurity posture to understand any gaps in compliance and develop a roadmap for remedy.

Implementation

Understanding any gap requirements, Wood will implement the necessary technical and organisational measures to ensure compliance.

Security maturity

Wood can oversee your security maturity roadmap and ongoing journey, from the initial assessment and implementation of remedial activities to continuous review and compliance.

Expertise

We have global industry leading cybersecurity specialists certified in ISO/IEC 27001 and IEC 62443, delivering services and support across multiple industries and sectors.

Wood is a global leader in consulting and engineering, delivering critical solutions across energy and materials markets. We provide consulting, projects and operations solutions in 60 countries, employing around 35,000 people.

For further information please go to:

woodplc.com   @Woodplc   Wood   @Woodplc   Wood