exeon

Smart Cyber Security.

WHITEPAPER

NIS2 Compliance Checklist:

Ensuring Network and Information Security

JUNE 2023

NIS2 Compliance Checklist:

Ensuring Network and Information Security

As the transition from the original NIS Directive to NIS2 is marked by several key changes and implications that organizations need to be aware of, the following checklist is meant to guide you through all the considerations and tools NIS2 requires.

1. UNDERSTAND THE SCOPE

Identify if your organization falls within the expanded scope of NIS2
NIS2 applies to any organization with more than 50 employees whose annual turnover exceeds €10 million and any organization previously included in the original NIS Directive.

The updated directive will also increase its scope to include the following new sectors:

- energy
- transport
- banking
- financial market infrastructure
- health
- drinking water supply
- digital infrastructure
- and public administration.

This expansion is in response to the increasing interdependence of these sectors and the potential cascading effects of cybersecurity incidents.
All 27 EU member states must incorporate the NIS2 Directive into their national laws by October 2024.

Table 1: NIS2 Industries Affected

PREVIOUS NIS SECTORS	ADDITIONAL NIS SECTORS
• Healthcare • Transportation • Water Supply • Energy • Virtual Infrastructure • Digital service providers • Banking • Financial market infrastructure	• Providers of public electronic communication networks or services • Wastewater • Chemicals • Healthcare (pharmaceutical, research and development, critical medical devices) • Food producers, processors and distributors • Critical product manufacturing (medical devices, computers, electronics, automobiles) • Digital vendors (social networking platforms, search engines, online marketplaces) • Aerospace • Postal and courier services • Public administration

If at this point, you are in scope, you must provide contact details:

- Notify ENISA of your entity name, addresses of main and other legal establishments in the EU.
- Provide up-to-date contact details, including email addresses and telephone numbers within 12 months.
- Foreign corporations not established in the EU but providing services (e.g., data center and content providers) must provide a designated representative contact.
- Update within 3 months when any change (of address or representative) becomes effective.

If you are not in scope, you can still participate and report significant incidents or cyber threats on a voluntary basis.

2. REVIEW THE KEY CHANGES AND IMPLICATIONS OF NIS2

2.1. Familiarize yourself with the transition from the original NIS Directive to NIS2 and the implications it has for your organization

As part of the new directive, critical entities must now:

- Initially report a significant security incident within 24 hours of discovery.
- Submit an initial assessment of the incident within 72 hours of discovery.
- Submit a detailed final report within one month of discovery.

2.2. Understand the stricter security requirements, including risk management practices and regular security assessments

According to Article 21 of the NIS2, member states should ensure that significant and important entities implement robust systems, policies, and best practices for managing risk that cover a variety of cybersecurity measures and disciplines, including:

- Risk analysis and security of information systems
- Incident handling and reporting
- Business continuity, e.g. backup management and disaster recovery
- Crisis management
- Supply chain security
- Security during system acquisition, development, and maintenance
- Basic cyber hygiene practices (see definition below) and cybersecurity training
- Cryptography and encryption technologies
- Personnel security, access control, and asset management
- Zero-trust access (multi-factor authentication, continuous authentication)
- Be aware of an increased emphasis on cooperation, information sharing, incident reporting.

"Cyber Hygiene" as per NIS2 Article 21

Cyber hygiene policies provide the foundation for protecting network and information system infrastructures, hardware, software, and online application security, as well as business and end-user data, upon which organizations rely on. Cyber hygiene policies, which encompass a common set of practices - including software and hardware updates, password changes, the management of new installations, the restricting administrator-level access accounts and securing data - enable a proactive framework of preparedness and overall security in the event of an incident or cyber threat.

3. ASSESS YOUR NETWORK AND INFORMATION SYSTEMS

3.1. Conduct a comprehensive assessment of your organization's network and information systems to identify potential threats and vulnerabilities

- **Assess your security posture:** a security assessment can help identify vulnerabilities such as unmanaged passwords or misconfigured or dormant accounts that are susceptible to credential to the theft of credentials.
- **Analyze your current ransomware defenses:** is your corporate network fully secured? Costly and crippling ransomware attacks are a major concern for EU regulators and one of the main reasons for the NIS2 directive. Implementing security solutions and best practices to proactively protect against ransomware.
- **Review your software supply chain:** supply chain attacks are a major concern for EU regulators and a key reason for the NIS2 directive. Take a fresh look at your software supply chain and consider implementing a Secrets Management solution to mitigate risks.

3.2. Evaluate the effectiveness of your current security measures and determine if they meet the requirements of NIS2

One of the security objectives of NIS2 is that data stored or transmitted electronically is protected from actions such as unauthorized access, modification, or deletion that may cause disruption to essential services. How effective is your organization in this regard?

Moreso, the organization must monitor the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and track the ongoing effectiveness of protective security measures.

For IT security-driven governance that covers IT and OT, make sure the operational site is included and collaborated with from early stages on. Without OT support, the cybersecurity initiative is not going to be effective.

Since organizations are required to report any significant cyber incidents that impact the security of their network and information systems to their designated national authorities, the reporting process should be timely and include sufficient information to enable the authorities to assess the incident and provide support where necessary.

4. IMPLEMENT RISK MANAGEMENT PRACTICES

4.1. Adopt a risk-based approach to network and information security

Do you have maximum visibility into your network, vulnerability mapping, risk assessment and reporting tools included?

4.2. Identify potential threats, assess their impact, and implement appropriate measures to mitigate risks

For budget and risk estimates, the ENISA NIS investment report can be of great use: consider outage costs and the loss of production, add the recovery and the efforts needed to get back to normal operations. Then, the estimated NIS2 penalty costs and damage to connected businesses will be demonstrated.

4.3. Regularly review and update your risk management practices to address the evolving threat landscape

5. DEVELOP AN INCIDENT REPORTING PROCESS

5.1. Create a process for reporting any significant cyber incidents that impact the security of your network and information systems

Since NIS2 encompasses incident reporting, make sure that the process consists of these steps:

- An incident or threat is identified
- Initial notification is sent by an entity within 24 hours
- Authorities sent an initial response within 24 hours and provide guidance on mitigation measures
- Intermediate report on relevant status updates sent by the entity on request by authorities
- A final incident report is sent by an entity (within one month after notification)

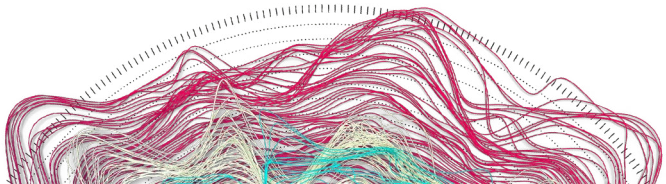
5.2. Ensure that the reporting is timely and includes sufficient information to enable the designated national authorities to assess and provide support if needed

6. ENSURE COMPLIANCE AND ENFORCEMENT

6.1. Familiarize yourself with the compliance and enforcement framework established by NIS2

Who and when to notify?

- The national competent authority or CSIRTs
- The recipients of the services (all incidents and potential incidents)
- Without delay, you must notify the parties within 24 hours following your realization of the incident
- A final incident report must be sent one month after the submission of the notification.



Your incident report must minimally include:

- A detailed description of the incident, its severity and impact
- The type of threat or root cause that likely triggered the incident
- The applied and ongoing mitigation measures
- Whether the incident is caused by unlawful or malicious action
- Proof that the cybersecurity risk management measures are defined and implemented
- The measures are approved by management bodies which are also held accountable for non-compliance
- Specific training to apprehend security risk and its impact on operations
- If non-compliance is detected, without undue delay, necessary corrective measures should be taken to bring the service concerned into compliance

6.2. Understand the potential sanctions and penalties for non-compliance

Member States may impose fines of up to EUR 10 million or 2% of annual turnover (revenue) for certain infringements or violations. In addition, critical management bodies (i.e. management teams) can be held personally liable for violations.

6.3. Be prepared for audits and inspections by national authorities to ensure you are meeting your obligations

7. CONSIDER NETWORK DETECTION & RESPONSE (NDR) SOLUTIONS

7.1. Evaluate the benefits of implementing NDR solutions for effective network monitoring and security

In order to address the challenges posed by NIS2 and ensure the security and resilience of their network and information systems, Network Detection and Response (NDR) solutions are indispensable for critical infrastructure operators.

NDR offers a number of benefits for organizations to comply with NIS2, including:

- **Visibility:** NDR solutions provide comprehensive visibility into network traffic, enabling organizations to identify potential threats and vulnerabilities before they can be exploited.
- **Detection:** By continuously monitoring network traffic, NDR solutions can detect and alert organizations to suspicious activity, such as unauthorized access attempts or data exfiltration.
- **Response:** NDR solutions enable organizations to respond quickly and effectively to potential threats by triggering incident response procedures.
- **Compliance:** NDR solutions can help organizations meet the reporting requirements under NIS2 by providing detailed logs and reports of network activity and incidents.

Overall, NDR serves as a key tool for critical infrastructure operators to comply with the updated NIS Directive and ensure the security and resilience of their network and information systems.

7.2. Assess the capabilities of NDR solutions, such as comprehensive visibility, detection of suspicious activity, incident response support, and compliance reporting

Book a free demo to discover how ExeonTrace leverages ML algorithms to make your organization more cyber resilient and NIS2 compliant – quickly, reliably and completely hardware-free.

8. CHOOSE A SUITABLE NDR SOLUTION PROVIDER

8.1. Select a reputable NDR solution provider that can meet your organization's specific needs

At Exeon, we understand the challenges faced by critical infrastructure operators in complying with the updated NIS Directive, or NIS2. Our Network Detection and Response (NDR) solution provides comprehensive visibility into network traffic, detects and alerts organizations to potential threats, enables effective response, and facilitates compliance with reporting requirements. Learn more about how we can help you ensure the security and resilience of your network and information systems at exeon.com.

9. REGULARLY REVIEW AND UPDATE YOUR SECURITY MEASURES

9.1. Ensure that your responsible staff is continuously overseeing the network monitoring and security measures

9.2. Stay informed about emerging threats and technological advancements in cybersecurity

9.3. Regularly update your risk management practices and technical measures to address new challenges

Remember that this checklist provides a general overview and should be adapted to your organization's specific needs and requirements. Click here for the full legislation published by the European Parliament.

NEXT STEPS

Contact us for a consultation on how ExeonTrace shields large enterprise networks and critical infrastructure. Our cybersecurity experts and engineers will show you the complete visibility of network data flows it provides and the automatic detection of suspicious behaviour, efficiently supporting your security team in responding to dormant and active threats – before any real damage is done.

Download the KuppingerCole Executive View on NDR for a deeper understanding of network monitoring as a foundational element of security architecture.

Sign up to our cybersecurity newsletter for the latest insights on NDR and events throughout the DACH region.

Those who trust ExeonTrace:

PostFinance SWISS PLANZER swisscom NTT DATA Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra

Exeon Analytics AG
Grubenstrasse 12
8045 Zürich, Switzerland

+41 44 500 77 21
contact@exeon.com
exeon.com

swiss made software

Gartner Peer Insights

Consistently rated 5/5 on Gartner – read the reviews here.

LinkedIn https://exeon.pub/linkedin

YouTube https://exeon.pub/youtube