asee by asseco

NIS2 ebook

NIS2 Checklist: 5 Steps To Kick Off Your Compliance Journey

Intro to NIS2

Cybersecurity is no longer a back-office concern - it's a front-line priority. With cyber-attacks growing more sophisticated and disruptive every day, the European Union has raised the bar with the **NIS2 Directive**.

NIS2 isn't just a refresh of the 2016 NIS Directive, it's a game-changer demanding security and resilience of digital ecosystems across the EU. The tight timeframe leaves entities with limited time to prepare, emphasizing the importance of starting their compliance journey now.

It is also important to mention that **the average timeline for organizations to reach full compliance is 12 months**, meaning, **the time to act is now**. Whether you're running a power grid, a hospital, or a manufacturing plant, NIS2 demands your attention, and consequently, action.

But what does compliance entail? How should organizations proceed? This eBook provides you with a NIS2 checklist of to-do's on your way to reach compliance.

https://cybersecurity.asee.io/nis2/

Contact us

asee
by asseco

What is the NIS2 Directive and who does it impact

The NIS2 Directive expands on its predecessor by broadening its scope and clarifying its requirements. It applies to two categories of organizations:

1. Essential Entities

These include sectors such as energy, transport, banking, financial market infrastructures, health, drinking water supply, and digital infrastructure. Disruptions to these sectors can have severe consequences on general society's well-being and economic stability.

Both categories face similar **requirements**, including the need to **implement security measures, conduct risk assessments,** and **report significant incidents**. However, essential entities are subject to stricter oversight, with regular audits and mandatory penalties for non-compliance.

2. Important Entities

These involves sectors like manufacturing of critical products, postal and courier services, waste management, food production, and chemicals. While not as critical as essential entities, these organizations also play vital roles in the economy and society.

https://cybersecurity.asee.io/nis2/

Contact us

The NIS2 checklist to reach compliance: 5 key stages

Achieving compliance with NIS2 is a multi-layered process. It requires organizations to assess their current cybersecurity posture, address gaps, and adopt an ongoing improvement strategy. Below are the five key stages that should be on your NIS2 checklist:

1. Business understanding, planning, and scoping

The first step in achieving NIS2 compliance is understanding how the directive applies to your organization. This involves identifying whether your entity falls under the "essential" or "important" category and determining the specific obligations concerning your sector.

During this stage, organizations must also map their business operations, network infrastructure, and digital assets. This ensures that all critical dependencies and vulnerabilities are identified. A thorough scoping process lays the foundation for creating a comprehensive compliance strategy.

Key actions

- **Assess organizational exposure to NIS2 obligations.**
- **Map critical systems, assets, and dependencies.**
- **Engage key stakeholders to align compliance goals with broader business objectives.**

2. Conducting gap analysis

Once the scope is defined, organizations need to perform a gap analysis to **compare their current cybersecurity practices against NIS2 requirements**. This process highlights deficiencies in areas such as incident reporting, risk management, and governance frameworks.

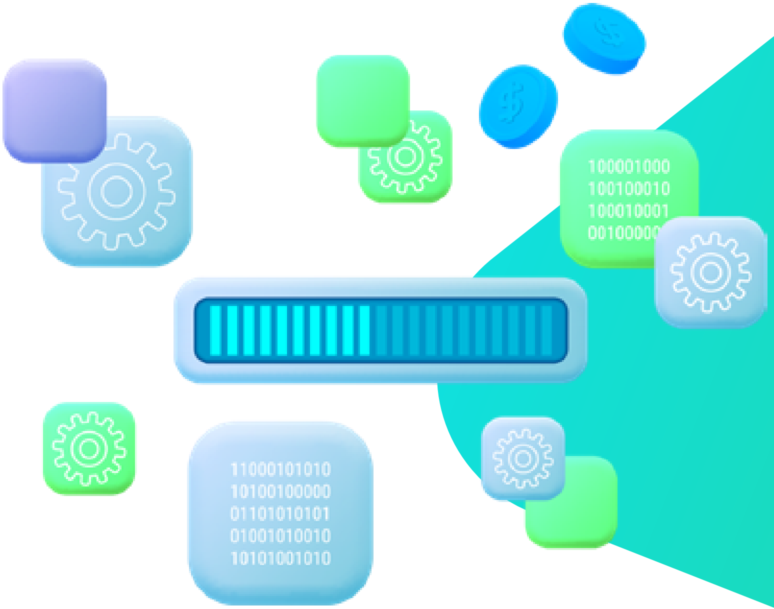
A thorough gap analysis includes a **review of existing policies, procedures, and technological controls**. It should also assess organizational readiness to meet incident reporting timelines and demonstrate accountability.

Key actions

- **Compare current practices with NIS2 requirements.**
- **Identify gaps in governance, risk management, and incident response.**
- **Prioritize areas for improvement based on risk impact.**

asee
by asseco

3. Defining a roadmap to close the gaps



With a clear understanding of existing gaps, organizations must create a detailed roadmap outlining how they will address them. This roadmap should prioritize critical vulnerabilities and align with available resources and timelines.

A well-defined roadmap provides a structured approach to achieving compliance. It should include milestones, responsible teams, and measurable success criteria to track progress. Aligning the roadmap with the organization's overall strategic goals ensures long-term sustainability.

Key actions

- **Develop a prioritized action plan for closing gaps.**
- **Assign responsibilities to relevant teams and individuals.**
- **Establish timelines and key performance indicators (KPIs) for tracking progress.**

4. Supporting implementation of cybersecurity measures

The next phase involves implementing the necessary security measures identified in the roadmap. This may include deploying new technologies, updating policies, and training staff on compliance-related responsibilities.

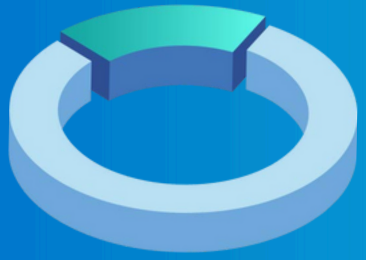
Organizations must focus on both technical and organizational measures to meet NIS2 standards.

Technical measures include enhancing network security, applying encryption, and establishing monitoring systems. **Organizational measures** involve fostering a culture of cybersecurity awareness and ensuring accountability at all levels.

Key actions

- **Implement and test technical controls such as firewalls and intrusion detection systems.**
- **Update policies to reflect NIS2 requirements, such as incident reporting and risk assessment procedures.**
- **Conduct staff training to build cybersecurity awareness and skills.**

5. Monitoring and improvement



Achieving compliance is not a one-time effort. Organizations must establish a process for continuous monitoring, auditing, and improvement. This involves staying updated on regulatory changes, conducting regular risk assessments, and adapting to emerging threats.

Monitoring systems should be put in place to track performance against compliance metrics. Incident response plans should be tested periodically to ensure effectiveness.

Key actions

- **Establish a monitoring framework for compliance and performance metrics.**
- **Conduct regular audits and risk assessments.**
- **Update security measures to address new vulnerabilities and regulatory changes.**

asee
by asseco

The path to compliance

For organizations, the path to compliance involves a structured journey: **understanding their business and obligations, identifying and addressing gaps, planning and implementing necessary measures, and continuously improving their cybersecurity posture**. While the process may seem complex, starting early and following a clear roadmap can help organizations meet national deadlines and beyond.

ASEE provides tailored solutions designed to help organizations address key NIS2 requirements. From advanced tools to enhance cybersecurity measures to solutions that support compliance efforts, we offer the resources you need to strengthen your security posture and meet regulatory demands.

NIS2 offer by ASEE

https://cybersecurity.asee.io/nis2/

In case you have any questions regarding the latest NIS2 Directive, we are happy to advise you and provide support along the way. Contact us and arrange your free, zero-obligation consultation.

Contact us