5 STEPS TO NIS2 COMPLIANCE

A How-To Guide

Business Challenge

As the deadline for transposing the NIS2 Directive into national law approaches on October 17, 2024, organizations falling under its purview must proactively prepare for compliance. Unlike EU regulations, NIS2, being a directive, is not directly binding, but sets a minimum standard. However, when your country implements national regulation attached to NIS2, your organization must take steps to be compliant to local law. Each country will create their own regulation attached to NIS2 and these will vary from country to country.

Follow these five crucial steps to navigate the complexities and ensure a smooth transition:

1. Involve your top management

The success of any compliance initiative relies on the backing of your organization's leaders.

- Inform the executive board about penalties outlined in the NIS2 Directive, emphasizing the liability of management bodies.
- Conduct educational sessions with senior executives to enhance their understanding of cybersecurity risk management issues and NIS2 requirements.
- Ensure top management approves and oversees cybersecurity risk management measures.
- Seek executive sponsorship to align actions with the board's expectations and expedite compliance processes.

2. Understand the Scope

Figuring out the scope of NIS2, your systems that fall under this scope, and challenges in achieving compliance are the first steps to achieving NIS2 compliance. Consider the following:

- Identify essential services provided by your organization.
- Determine if your organization qualifies as an essential or important entity in your country.
- Evaluate the need for new security measures to meet compliance.
- Consider the impact on suppliers, partners, or customers subject to the Directive.
- Include NIS2 compliance obligations in contract agreements with relevant entities.
- Take into account your organization's size, focusing on medium and large organizations within critical sectors.

3. Study the NIS2 security requirements

Familiarize yourself with Article 21 of the Directive, outlining the main NIS2 requirements.

Ensure your organization addresses the ten security measures mandated by NIS2, ranging from risk analysis to multi-factor authentication.

1. Policies on risk analysis and information system security
2. Incident handling
3. Business continuity, such as backup management and disaster recovery, and crisis management
4. Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
5. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
7. Basic cyber hygiene practices and cybersecurity training
8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption
9. Human resources security, access control policies and asset management
10. The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications, and secured emergency communication systems within the entity, where appropriate.

Recognize that specific laws and regulations transposed from NIS2 may vary among Member States.

4. Conduct gap analysis

Once you've identified the scope and requirements of NIS2, you're ready to compare them to the existing security measures implemented in your organization. Gap analysis bridges any existing gaps between the current state of compliance and the desired one.

For a proper gap analysis, take the following key steps:

- Define the scope and requirements for the gap analysis.
- Set desired benchmarks for compliance.
- Assess the current state of cybersecurity within your organization.
- Cross-reference existing cybersecurity measures with NIS2 requirements.
- Identify and prioritize compliance gaps.
- Develop a comprehensive action plan with clear goals and deadlines.
- Consider conducting regular gap analysis to adapt to evolving cybersecurity requirements.

5. Allocate the necessary resources

Successful implementation of the NIS2 Directive requirements involves allocating the resources needed, including money, people, and technology:

- Estimate the budget for compliance activities, gaining executive approval and avoiding unexpected expenses.
- Assemble a dedicated team responsible for compliance, specifying roles and responsibilities.
- Invest in security technology to address identified gaps, exploring automation tools for streamlined compliance processes.

Complying with NIS2 will likely require the implementation of cybersecurity software solutions. See how Tenable can help you align your needs in the next section.

How Tenable Helps with NIS2 Alignment

An effective exposure management program helps organizations gain visibility across the modern attack surface, focus efforts to prevent likely attacks, and accurately communicate cyber risk to support optimal business performance.

While the above steps can help you begin to navigate the complexities that this new directive brings, there are other considerations that organizations must consider while preparing and implementing policies aligned with NIS2. Tenable offers a feature-rich toolset to enhance cyber resilience and addresses many NIS2 requirements effectively, providing a comprehensive solution for organizations navigating the complexities of compliance. Tenable can help your organization with compliance readiness across vulnerability management, identity security, cloud security, and more.

For more information on how Tenable can help your organization, check out our Tenable Products and NIS2 Directive solutions pages.

ABOUT TENABLE

Tenable® is the Exposure Management company. Approximately 43,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at tenable.com.

For More Information: Please visit tenable.com
Contact us at sales@tenable.com or visit tenable.com/contact