NIS2 QUALITY MARK

The cyber security standard applied to the supply chain

This is an outdated version.
A new version will be available on Wednesday, October 16.

NIS2 QUALITY MARK

The cyber security standard applied to the supply chain

Article 21.2d of the European NIS2 Directive imposes cyber hygiene requirements on critical industries, services and infrastructure. Essential and important companies must therefore collaborate with their direct suppliers to ensure the security of the supply chain. The NIS2 Quality Mark provides a suitable standard for this with three levels (Basic, Substantial, and High), to match measures with the appropriate threat levels.

NIS2 Quality Mark Basic: NIS2 QM10		Mapping* with ISO27001
1. Organisational control measures		
1.2	**Policy development for information security and executive approval:** Formulate a plan for cybersecurity and ensure it is safeguarded. The plan must include at least a set of basic guidelines for cybersecurity, such as updates, password changes, installation management, restricting access levels, and data backups. The responsibilities for initiating and deciding on all cybersecurity measures must be clearly defined. Always ensure approval from senior management and communicate the plan to all relevant employees.	A.5.1
1.3	**Assignment of responsibility in information security:** Define tasks and responsibilities in cybersecurity and assign them. The responsibilities for initiating and deciding on all cybersecurity measures must be clearly defined. Appoint at least one person who is responsible for the organisation's cybersecurity.	A.5.2
1.6.1	**Overview of information:** Create and maintain a list of all company information, including customer information and contracts. Assign an owner (administrator) to each asset.	A.5.9
1.6.2	**Overview of ICT assets:** Create and maintain a list of all ICT assets, including software, servers, data storage systems, and firewalls. Also, assign a responsible owner (administrator) to each asset.	A.5.9
1.8	**Returning company assets after use:** Ensure that, using a procedure and a checklist, employees return company assets (such as computers and smartphones) upon departure. This safeguards the confidentiality of stored information.	A.5.11
1.14	**Granting and management of access rights:** Implement a procedure to prevent new employees from obtaining unauthorised access rights and to ensure that accounts are properly deactivated upon termination of employment. Maintain a record indicating who has received logical and physical access rights and the date on which these rights were revoked.	A.5.18
1.23	**Preparation and optimisation of ICT for the business continuity process:** Develop a plan to respond to unexpected events, such as a cyber attack, and to quickly resume operations. The plan should include objectives and related continuity requirements, such as a backup management process, contingency plans, and crisis management.	A.5.30

**Mapping: This standard is similar, but not identical to ISO 27001. Each standardization system has its own specific characteristics.*

NIS2 Quality Mark Basic: NIS2 QM10		Mapping* with ISO27001
1. Organisational control measures		
1.26	**Securing the supply chain together:** Conduct a risk assessment for key suppliers, identify cybersecurity risks (related to the products or services being procured), and establish mutual agreements on digital security. Ensure that suppliers are also informed about the control measures they can take in the event of a cyber threat within the organisation.	n/a**
2. Human-oriented control measures		
2.2	**Education of executives and employees and awareness for securing information:** Ensure that executives and directors take a course or training to enable them to identify and assess cybersecurity risks. It is important that everyone in the organisation understands the risks associated with information processing. Use, for example, video training modules for employees on digital security. Employees must receive education and training on digital security appropriate to their role, and they should be tested on their knowledge of the organisation's policies and procedures.	A.6.3
2.6	**Working remotely in a secure manner:** Working outside the organisation increases the risk of a cyber incident. Formulate rules for secure information processing at external locations and ensure that all employees are aware of and comply with these rules.	A.6.7
2.7	**Recording and reporting incidents related to information security:** Make it clear to all employees how observed or suspected information security incidents can be quickly reported, recorded, and communicated through the appropriate channels.	A.6.8
3. Physical control measures		
3.9	**Access security measures:** Prevent unauthorized physical and logical access to assets containing sensitive information. Formulate access security rules that take into account business and information security requirements.	A.5.15
4. Technological control measures		
4.1	**Security and management of user devices:** To prevent cyber incidents, devices used by employees must be secured against unauthorized use, unauthorized software installation, and unauthorized changes to security settings. Advise employees on the proper handling of authentication information, such as passwords and PIN codes.	A.8.1
4.4	**Combating and preventing malware:** Take measures to protect the digital environment against malware, such as installing anti-malware software that detects and blocks malware, a virus scanner, and a spam filter.	A.8.7

*Mapping: This standard is similar, but not identical to ISO 27001. Each standardization system has its own specific characteristics.
** N/a: Not available, not applicable. There is no corresponding measure in ISO 27001.

NIS2 Quality Mark Basic: NIS2 QM10		Mapping* with ISO27001
4. Technological control measures		
4.5	**Information retention: backup and recovery:** Develop a backup plan (according to the 3-2-1 methodology), regularly create backups of important data and systems, and periodically test these for reliability.	A.8.13
4.7	**Keeping software on company assets up to date:** Keep company assets such as computers and other devices secure with regular updates. Install all updates immediately according to the established procedures for safe updating on all devices.	A.8.19
4.10	**Authentication on critical systems:** Ensure that the authentication methods used (such as passwords or MFA) align with the sensitivity of the information being accessed. MFA must be implemented, at a minimum, for accounts with administrative rights, accounts with access to systems containing business-sensitive information, and for users logging in via the internet.	A.8.5

**Mapping: This standard is similar, but not identical to ISO 27001. Each standardization system has its own specific characteristics.*

Copyright

Explanation on mapping

Our cybersecurity standard is the result of extensive collaboration between a diverse team of experts in the field of cybersecurity. This multidisciplinary team comprised representatives from NIS2 organisations, SMBs, independent cybersecurity specialists, and auditors. Through this varied composition, we ensured that our standard encompasses a wide range of perspectives and expertise, leading to a unique and highly valuable approach to cybersecurity.

While our standard may exhibit some overlap with other cybersecurity standards in certain areas, users should understand that our standard is a standalone product, developed with the specific needs and challenges of modern businesses in mind. The content and approach of our standard may therefore differ from that of other standards, even if there is some resemblance.

It is important to emphasize that our standard is designed to encompass best practices in cybersecurity, based on the insights and experiences of our diverse team members. Therefore, users should consider our standard as a unique tool developed for maximum added value and effectiveness for organisations striving for enhanced cybersecurity.

Disclaimer

While the measures included in the NIS2 Quality Mark and related overview of measures have been developed by experts and compiled with the utmost care, no guarantees are provided regarding the accuracy, completeness, reliability, suitability, or availability of the NIS2 Quality Mark and the information, products, services, or related graphics contained therein. The use of the NIS2 Quality Mark and related overview of measures is entirely at the user's risk. Any liability for damages, direct or indirect, arising from or in any way related to the use of the NIS2 Quality Mark and related overview of measures is excluded.

In the NIS2 Quality Mark mapping overview, references may be made to other standards, including ISO 27001 and NEN 7510, solely for informational purposes and to identify potential correlations or overlaps. These references do not imply any association, endorsement, or approval of the content of the other standards. The NIS2 Quality Mark and related overview of measures, as well as the mentioned other standards, are separate and unique documents. All rights related to other standards mentioned in the document belong to the respective rightful owners of those standards.

The NIS2 Quality Mark and related overview of measures are subject to copyright. No part of this standard may be reproduced, stored in an automated data file, or disclosed, in any form or by any means, electronically, mechanically, by photocopying, recording, or any other way, without prior written permission.