NIS2
QUALITY MARK

The Cybersecurity Standard for the Supply Chain

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

This is the NIS2-QM10 Basic standard, belonging to the NIS2 Quality Mark, an integral part of the Compliance and Certification Scheme of NIS2 Quality Mark and the Stichting Kwaliteitsinnovatie.

NIS2 Quality Mark Basic: NIS2 QM10		Mapping* with ISO27001
1. organisational control measures		
1.2	**Information security policy formulation and management approval:** The organisation's management should formulate a policy that sets out strategic objectives for protecting the availability, integrity and confidentiality of information from cyber threats. The policy is approved by management and communicated to relevant employees. The organisation shall formulate specific policies based on the cyber security strategy that support proactive preparedness and protection against incidents and cyber threats. The policies shall provide clarity on standard practices such as access security, application management, IT management, network management and backup management. The policies shall be approved by appropriate management and communicated to relevant employees.	**A.5.1**
1.3	**Assignment of responsibility for information security:** The organisation must define and assign tasks and responsibilities for cybersecurity. The responsibilities for initiating and deciding on cybersecurity measures are known to those responsible. At least one individual should be designated as the person accountable for the whole of the organisation's cybersecurity efforts.	**A.5.2**
1.6.1	**Information Overview:** The organisation must establish and maintain an overview of business information categories. For each category, an owner (manager) is designated to ensure the protection of the information within that category.	**A.5.9**
1.6.2	**ICT Assets Overview:** The organisation must establish and maintain an ICT assets overview, including servers, data storage systems and firewalls. For each asset (or group of assets), a designated owner (manager) is appointed, who is responsible for its protection.	**A.5.9**
1.8	**Returning company assets after use:** The organisation must use a procedure and checklist to ensure that employees and temporary workers return company assets (such as laptops, telephones, key cards and keys) after termination or change of their employment, contract or agreement.	**A.5.11**
1.14	**Access Privilege Management:** The organisation shall implement a procedure to ensure that access rights are properly granted, modified, and removed. Records shall be maintained showing who has been granted logical and physical access rights and the date on which they were revoked.	**A.5.18**
1.23	**ICT preparation for business continuity:** The organisation must develop a plan that includes ICT continuity requirements, including objectives for the maximum recovery time of essential information systems. Technical and organisational measures are implemented to meet the ICT continuity requirements in the event of a disruption.	**A.5.30**

**Mapping: This standard is similar, but not identical to ISO27001. Each standardisation system has its own specific characteristics. The 'A' referred to is the numbering from Appendix A of the 27001 standard.*

NIS2 Quality Mark Basic: NIS2 QM10		Mapping* with ISO27001
1. organisational control measures		
1.26	**Securing the supply chain together:** For the supply chain, the organisation shall take appropriate and proportionate technical, operational and organisational measures to prevent risks to the security of network and information systems. The measures for the supply chain must be based on an approach that encompasses all hazards related to the protection of networks, information systems, and the physical environment. The organisation must identify business risks associated with the use of products and services from suppliers in its policy. Relevant and proportionate agreements regarding digital resilience within the supply chain must be made with suppliers. The organisation shall document this policy in writing and demonstrably apply it.	A.5.21
2. People-oriented control measures		
2.2	**Cybersecurity education for directors and employees:** The organisation's directors and officers should receive training or instruction to help them identify and assess cybersecurity risks. Employees of the organisation should receive cybersecurity education and training appropriate to their roles and should be tested on their knowledge of the organisation's rules and procedures.	A.6.3
2.6	**Working from home or hybrid in a safe way:** The organisation must formulate and communicate rules for safe information processing at remote locations. The organisation ensures that all employees know the rules for working at remote locations.	A.6.7
2.7	**Information Security Event Reporting:** The organisation shall make it clear to all employees how to report observed or suspected information security events promptly and through appropriate communication channels.	A.6.8
3. Physical control measures		
3.9	**Define Access Control:** Based on predefined roles, the organisation should determine the access rights appropriate to each role, limited to the needs of that role.	A.5.15
4. Technological controls		
4.1	**Security and management of user devices:** Corporate devices used by employees and contractors (such as PCs, laptops, phones and tablets) must be secured against unauthorised use, unauthorised installation of software and unauthorised changes to security settings.	A.8.1
4.4	**Malware Control and Prevention:** The organisation shall implement anti-malware measures, including technical measures for the timely detection and neutralisation of malware.	A.8.7

**Mapping: This standard is similar, but not identical to ISO27001. Each standardisation system has its own specific characteristics. The 'A' referred to is the numbering from Appendix A of the 27001 standard.*

NIS2 Quality Mark Basic: NIS2 QM10		Mapping* with ISO27001
4. Technological controls		
4.5	**Backup and recovery:** Backups of information and systems should be made according to a defined backup plan. Backups are tested to ensure they are valid when they are needed.	A.8.13
4.7	**Keeping software on assets up to date:** The organisation shall define and implement a policy for keeping software on all assets up to date and secure at all times.	A.8.19
4.10	**Implement authentication methods:** The organisation must ensure that the authentication methods used are appropriate for the sensitivity of the information being accessed. At a minimum, MFA must be implemented for accounts with administrative rights, when accessing systems with sensitive information, and for all users who log in via the Internet.	A.8.5

**Mapping: This standard is similar, but not identical to ISO27001. Each standardisation system has its own specific characteristics. The 'A' referred to is the numbering from Appendix A of the 27001 standard.*

Copyright

This document is dynamic in nature. This is the version of 08-04-2025. Please consult the most recent version at www.nis2qualitymark.eu.

Explanation of mapping

Our cybersecurity standard is the result of extensive collaboration between a diverse team of cybersecurity experts. This multidisciplinary team included representatives from NIS2 organisations, SMEs, independent cybersecurity specialists, and auditors. This diverse composition ensured that our standard encompasses a wide range of perspectives and expertise, resulting in a unique and highly valuable approach to cybersecurity.

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

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

Disclaimer

Although the measures included in the NIS2 Quality Mark and related overview of measures have been developed by experts and have been compiled with the greatest possible care, no guarantees are given as to the correctness, completeness, reliability, suitability, or availability with respect to 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 risk of the user. Any liability for damage, direct or indirect, arising out of or in any way connected with the use of the NIS2 Quality Mark and related overview of measures is excluded.

The NIS2 Quality Mark mapping overview may contain references to other standards, including ISO 27001 and NEN 7510, for information purposes only and to identify possible connections or areas of overlap. These references do not imply any association with or endorsement of the contents of the other standards. The NIS2 Quality Mark and related overview of measures and the other standards mentioned are separate and unique documents. All rights with respect to other standards mentioned in the document belong to their respective owners.

The NIS2 Quality Mark and related summary of measures are protected by copyright. No part of this standard may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission.