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-QM20 Substantial 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 Substantial: NIS2 QM20		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 is designated as the primary person accountable for the whole of the organisation's cybersecurity.	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, responsible for safeguarding 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 assigned, responsible for its protection.	A.5.9
1.7	**Acceptable use of information and related assets:** The organisation shall establish and communicate rules for the safe use of information and related assets such as computers, laptops, telephones, storage media and business applications.	A.5.10
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
1.9	**Classifying information:** The organisation must maintain an overview of different categories of business information that have the same level of confidentiality in a classification scheme. For each category, it has been determined how the business information in question must be treated and protected to ensure its confidentiality. For each category, it has also been determined whether the business information in question must be labeled to make it more recognisable to employees.	A.5.12

**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 Annex A of the 27001 standard.*

NIS2 Quality Mark Substantial: NIS2 QM20		Mapping* with ISO27001
1. organisational control measures		
1.13	**User Registration and Deregistration:** The organisation shall define and implement a procedure for creating, modifying and timely deleting of all types of accounts used by registered employees and temporary workers.	A.5.16
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
1.15	**Protection of information in cooperation with suppliers:** The organisation must define processes and procedures that enable the organisation to determine whether services and products from suppliers sufficiently meet the information security requirements of the organisation. If necessary, appropriate measures are taken to manage the risks.	A.5.19
1.20	**Guidelines for dealing with information security incidents (cybersecurity incidents):** A plan should be drawn up that clearly states how the organisation deals with a suspected or confirmed breach of the availability, integrity or confidentiality of information. The plan clearly states who is responsible for each task.	5.24
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
1.26	**Securing the supply chain together:** The organisation must determine the information security risks associated with the use of ICT products and ICT services from suppliers, or from suppliers further down the supply chain. Relevant agreements regarding information security in the ICT supply chain have been agreed with the organisation's suppliers.	A.5.21
1.27	**Collecting evidence:** The organisation must determine for which types of incidents which evidence must be collected and secured in order to determine the cause or to provide evidence to third parties.	A.5.28 /5.29
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

**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 Substantial: NIS2 QM20		Mapping* with ISO27001
2. People-oriented measures		
2.6	**Working from home and 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	**Recording and reporting of information security events:** The organisation shall make it clear to all employees how observed or suspected information security events can be reported promptly and through appropriate communication channels.	A.6.8
3. Physical control measures		
3.5	**Confidential Policy regarding Desks and Screens:** The organisation shall formulate and communicate policies for locking active computer screens and removing paper and storage media containing confidential information from unattended workstations. The organisation shall ensure that all employees are aware of and comply with the policies for unattended workstations.	A.7.7
3.8	**Safely Dispose or Reuse Corporate Devices:** The organisation must define and implement a process for the safe disposal or reuse of corporate devices that contain embedded storage media. The rules make it clear that sensitive data and software must be deleted or overwritten before a corporate device can be disposed of or reused.	A.7.14
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
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

**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 Substantial: NIS2 QM20		Mapping* met ISO27001
4. Technological controls		
4.9	**Network Segmentation:** The organisation shall establish and implement rules for segmenting groups of users, information systems, and information services in the organisation's networks.	A.8.22
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
4.11	**Log files:** The organisation shall record and analyse log files of relevant events. Based on a risk assessment, the organisation has determined what are relevant events and how the recorded log files should be analysed.	A.8.15

**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.*

The cybersecurity standard for the supply chain

Below are some additional controls that apply specifically to organisations that work in or use Operational Technology (OT) and Information Technology (IT). Of course, the general controls above also apply to these companies.

NIS2 Quality Mark Substantial: NIS2 QM20		Mapping* with ISO27001
OT control measures		
5.1	**Register of all OT assets:** The organisation shall establish and maintain a list of OT assets, including relevant configuration data, such as software versions and patch levels. An owner (manager) shall be appointed for each asset.	n/a**
5.2	**Determine the dependency on OT assets:** The organisation must define for each OT asset how dependent the organisation is on it, what the probability of failure is, and what the impact is in the event of a failure.	n/a
5.4	**Backups of OT systems:** Backups of OT systems should be made according to a defined backup plan. Backups are tested to ensure they are valid when they are to be used.	n/a
5.5	**Recovery plan OT systems:** The organisation must develop a business continuity plan that includes continuity requirements for disruptions, including the accepted recovery time of essential OT systems. Technical and organisational measures are implemented to meet the OT continuity requirements in the event of a disruption. The effectiveness of these measures has been tested.	n/a
5.11	**OT system overview and additional information:** The organisation shall establish and maintain an overview of all OT systems, including information on hardware, software, firmware, configurations, security settings, suppliers and maintenance. An owner (manager) is appointed for each OT system.	n/a
IT management measures		
6.1	**Access to source code:** The organisation shall protect access to source code and software libraries from unauthorised access and unwanted modification.	8.4
6.3	**Developing secure software:** The organisation shall establish best practices for developing secure software. Compliance with these best practices shall be monitored.	A.8.27
6.9	**Software Delivered Overview:** The organisation must establish and maintain an overview of all customers who use software created by the organisation. This overview should clearly indicate which customer is using which version of each software product.	n/a
6.12	**Customer coordination of new software and updates:** The organisation shall define and implement a process for installing new software versions or patches in consultation with customers.	n/a

**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.*

*** N/a: Not available, not applicable. There is no corresponding measure in ISO27001.*

Copyright

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 regarding 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.