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-QM30 High 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 High: NIS2 QM30		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
1.4	**Management Direction:** The organisation's management must explicitly require all employees, including all new employees, to work in accordance with the organisation's information security policies and procedures.	A.5.4
1.5	**Security Threat Assessment and Understanding:** The organisation should regularly consult appropriate sources to stay informed about threats that may be relevant to information security. Additional measures are taken as needed to protect against new or changing threats.	A.5.7
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

**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 High: NIS2 QM30		Mapping* with ISO27001
1. organisational control measures		
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
1.11	**Transferring information within the organisation and to third parties:** The organisation must establish rules that make clear which resources and external parties may be used for the secure transfer of confidential information within the organisation, and between the organisation and other parties. The organisation ensures that employees are aware of the rules for transferring information.	A.5.14
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
1.16	**Ensuring information security in agreements with suppliers:** The organisation must define processes and procedures that enable the organisation to determine whether the guarantees offered by suppliers sufficiently meet the information security requirements of the organisation. If necessary, additional agreements are agreed upon.	A.5.20
1.18	**Supervision, evaluation and change management of supplier services:** The organisation must use a risk assessment to decide which service suppliers need extra monitoring. These selected suppliers are regularly evaluated to check if the reliability and security of their services meet both the agreed-upon terms and the organisation's current requirements.	A.5.22

**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 High: NIS2 QM30		Mapping* with ISO27001
1. organisational control measures		
1.19	**Keeping information secure when using cloud services:** The organisation shall define processes that enable the organisation to determine whether safeguards provided by cloud service providers adequately meet the organisation's information security requirements.	5.23
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
1.21	**Recording, assessment and handling of information security incidents:** The organisation shall assess events relating to information security to determine whether they constitute incidents. Incidents relating to the availability, integrity or confidentiality of information shall be recorded and handled in accordance with documented procedures.	5.25
1.22	**Incident reporting to external parties:** The organisation has and uses a documented procedure to report incidents relating to the availability, integrity or confidentiality of information to external parties, in accordance with legal and contractual requirements.	5.26
1.23	**ICT preparation for business continuity:** The organisation must develop a business continuity 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
1.24	**Objective assessment of the information security approach:** The organisation must conduct an independent assessment at planned intervals to determine whether the information security approach is sufficiently meeting the information security objectives as set out in the information security policy. If it is found that the strategy is inadequate, management will take corrective measures.	5.35
1.25	**Independent assessment of information security:** The organisation must conduct an independent assessment at planned intervals to determine whether the organisation is operating in accordance with the requirements of the NIS2 Quality Mark standard, and in accordance with the organisation's own information security requirements in the form of internal rules, agreements, processes and procedures.	5.36

**Mapping: This standard is similar, but not identical to ISO27001. Each standardisation system has its own specific characteristics.*

The cybersecurity standard applied to the supply chain

NIS2 Quality Mark High: NIS2 QM30		Mapping* met ISO27001
1. organisational control measures		
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		
2.1	**Confidentiality obligation in employment contracts:** All forms of employment contracts must include a confidentiality obligation.	A.6.2
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
2.4	**Ongoing confidentiality obligations after termination or change of employment relationship:** It must be agreed with employees and temporary workers that a duty of confidentiality continues to apply after termination or change of their employment, contract or agreement.	A.6.5
2.5	**Confidentiality agreements:** The organisation must ensure that employees and contractors sign a confidentiality agreement, which stipulates that confidential information exchanged during the collaboration may not be disclosed to third parties.	A.6.6
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

**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.*

NIS2 Quality Mark High: NIS2 QM30		Mapping* with ISO27001
2. People-oriented control measures		
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
2.8	**Background checks on candidates for employment:** The organisation shall establish and implement rules for conducting background checks on candidates for employment prior to their employment with the organisation. The scope and thoroughness of these checks will align with the information security risks related to the specific roles being filled.	A.6.1
3. Physical control measures		
3.1	**Physical access security:** The organisation shall design and implement appropriate physical security for sites, buildings, offices and spaces based on a risk assessment. The design shall take into account the organisation's need to be able to grant or prevent specific access within an environment.	A.7.1/ A.7.2
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

**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 High: NIS2 QM30		Mapping* with ISO27001
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
4.2	**Special Access Privileges:** The organisation shall implement a procedure to ensure that special access rights, such as system and application administrator access rights, are properly granted, modified, and removed. Records shall be maintained showing who has been granted special access rights and the date on which they were revoked.	A.8.2
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
4.6	**Redundant implementation of ICT infrastructure:** The organisation must determine which parts of the ICT infrastructure require redundancy based on business continuity objectives and ICT continuity objectives (see 1.23). These redundant implementations must be deployed and tested to ensure they meet continuity objectives.	A.8.14
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
4.8	**Manage and secure networks:** The organisation must define and assign responsibilities for managing and configuring networks and network devices. All network devices are listed in an inventory and have an owner (administrator). The inventory is maintained and contains relevant information about the network devices.	A.8.20
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

**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 High: NIS2 QM30		Mapping* with ISO27001
4. Technological controls		
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
4.12	**Cryptography and encryption:** Based on a risk assessment, the organisation should establish and implement rules that clarify in which cases stored and transmitted information must be secured with a specific form of cryptography. These rules also clarify how cryptographic keys must be stored securely.	A.8.24
4.14	**Finding and repairing technical vulnerabilities in a timely manner:** The organisation shall define and assign responsibilities for the timely finding, recording and repairing of technical vulnerabilities in networks and information systems under the organisation's management.	A.8.8
4.15	**Controlled implementation of changes:** The organisation shall define and implement a process for the controlled implementation of changes to networks and information systems under the organisation's control. The process shall include a mandatory analysis of the potential impact on the availability, integrity and confidentiality of information.	A.8.32

**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.*

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 High: NIS2 QM30		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
5.6	**Segmentation of OT networks:** The organisation shall establish and implement rules for segmenting the organisation's OT networks.	n/a
5.8	**Remote access to critical OT systems:** The organisation shall use a server that acts as a secure access point for remote access to critical OT systems under the organisation's control. The server in question shall have an owner (administrator) who is responsible for its security.	n/a
5.9	**Installing OT Patches:** The organisation shall establish and assign responsibilities for the timely application of critical patches to systems within OT networks under the organisation's management.	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

**Mapping: This standard is similar, but not identical to ISO27001. Each standardisation system has its own specific characteristics.*
*** N/a: Not available, not applicable. There is no corresponding measure in ISO27001.*

NIS2 Quality Mark High: NIS2 QM30		Mapping* with ISO27001
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
6.2	**Keeping the program code and external components up to date:** Organisations that develop applications must ensure that program code, including external components such as libraries and frameworks, is regularly updated with the latest security updates. This is documented in a formal process, with updates performed and documented within a set timeframe. The process is periodically evaluated and checked for compliance.	n/a
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
6.4	**Information Security Awareness in Application Development:** Organisations that develop applications should ensure that developers are aware of the information security risks associated with developing applications and using those applications to process information.	A.6.3
6.5	**Testing the security of applications:** Organisations that develop (or have developed) applications must first set requirements for the security of the applications with a view to their use in practice. When testing a developed application, not only the user aspects are tested, but also the security aspects of the application.	A.8.29
6.6	**Outsourced software development:** When the development of custom software is (partly) outsourced to an external party, the organisation actively monitors the development activities and determines whether the delivered software meets the information security requirements.	A.8.3
6.7	**Separation of development, test, acceptance and production:** Organisations that develop applications (or have them developed) must ensure that development and test environments remain separate from production environments, for example by using separate virtual or physical environments, in combination with separate access rights.	A.8.31
6.8	**Procedures and methods for deploying software:** Organisations that install or have software installed on their operational systems must implement procedures and measures to do this in a safe and controlled manner.	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.*

NIS2 Quality Mark High: NIS2 QM30		Mapping* with ISO27001
IT management measures		
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
6.10	**Maintaining an overview of delivered equipment and software:** The organisation must maintain an accurate inventory of all equipment and software delivered to customers and record it in an up-to-date and documented overview of the IT landscape. This overview should be reviewed and updated periodically. The process must ensure that proactive maintenance is carried out and that security updates are applied to customers in a timely manner.	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.*

*** 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.