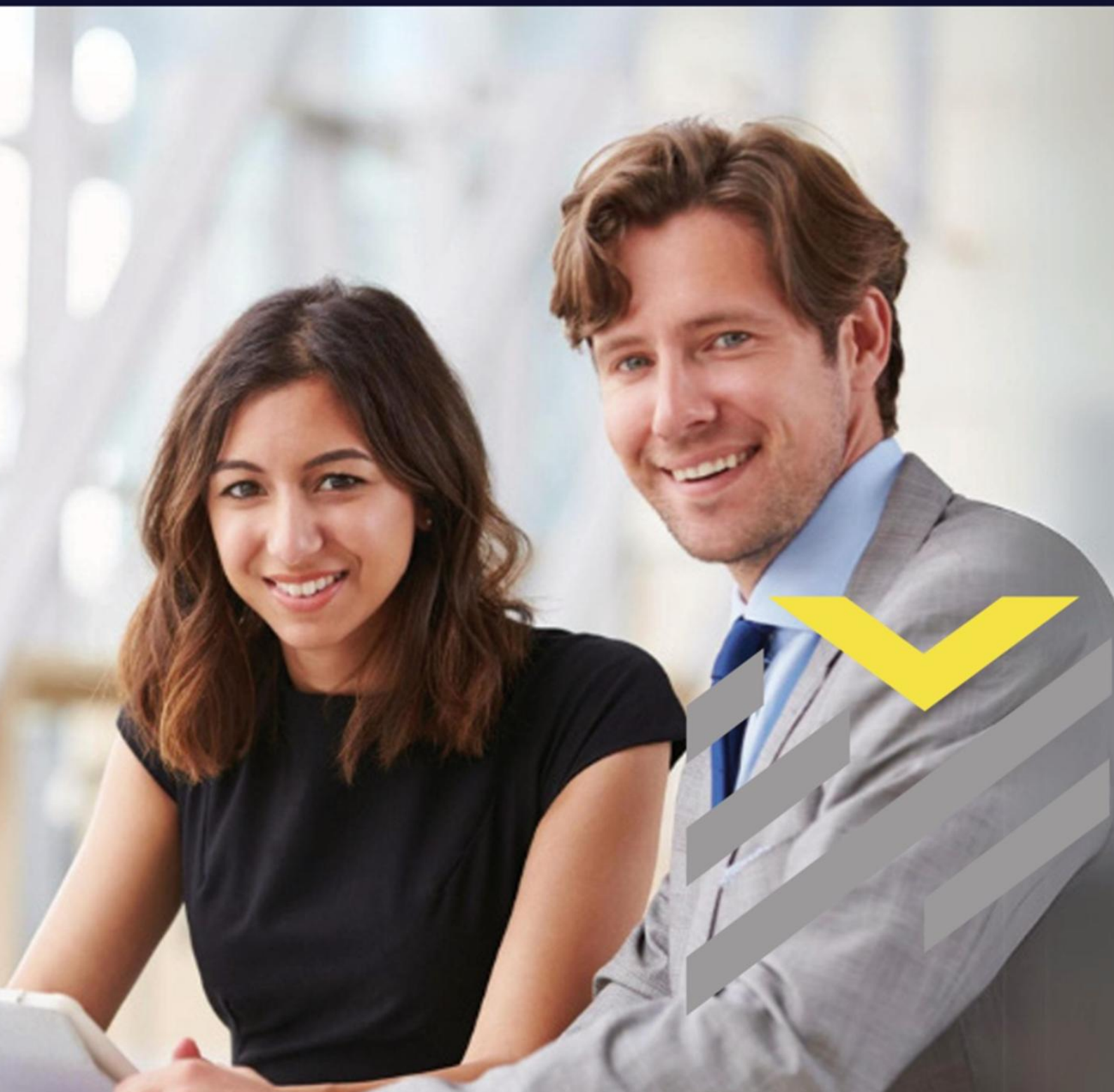
NIS2 Supply Chain

Compliance and Certification scheme

Version 3.2
January 1, 2026



Foreword

The NIS2 (Network and Information Security) directive of the European Union is an extension and replacement of the original NIS directive. The aim of NIS2 is to strengthen the digital and operational resilience of essential and important se ctors within the EU. The directive sets stricter security requirements and reporting obligations for organisations to better prevent, detect and address cyber threats more effectively. This includes all essential and important NIS2 entities, as well as their direct suppliers.

This document is the working translation of the Compliance and Certification Scheme from the Dutch language.

Article 21.2(d) of the NIS2 Directive focuses on the security of the supply chain through the direct suppliers of products and services. This article requires organisations within the scope of NIS2 to take appropriate measures to ensure that their direct suppliers and service providers also comply with the relevant security requirements.

This means that these organisations are responsible for ensuring the cybersecurity of their supply chain (direct suppliers). They must monitor and verify that suppliers and service providers have implemented adequate security measures to minimize cyber risks. This means that organisations:

- Must work with suppliers to improve security practices and coordinate incident response procedures to ensure business continuity in the event of cyber incidents.
- By taking these measures, they improve the security of their entire supply chain and reduce the likelihood of cyber incidents by including in contracts that suppliers must meet specific security standards.
- Audits and/or diagnoses and/or assessments must be carried out (or have them carried out) to check the compliance of suppliers with security measures.
- Periodic risk assessments should be conducted of vendors to identify potential vulnerabilities and threats.

The supply chain includes not only large companies but also many small and medium-sized companies (SMEs). They have their own challenges when it comes to increasing their cybersecurity:

- SMEs often have limited budgets and limited in-house cybersecurity expertise.
- They often do not have their own specialized ICT and/or cybersecurity staff.
- SME employees are often less aware of cybersecurity risks and may not have received the necessary training to recognize and respond to cyber threats.
- Understanding and complying with complex regulations like NIS2 can be difficult for SMEs, especially without the help of legal and compliance experts.

The Foundation for Quality Innovation ('Stichting Kwaliteitsinnovatie')

This Compliance and Certification Scheme has been drawn up by the Foundation for Quality Innovation. As a Foundation, which works for the interests of cooperating industry and professional organisations and the companies and professionals affiliated there, we strive to improve cybersecurity for all companies and organisations in Europe. We do this by making a widely supported standard accessible at several levels. We deliberately choose relevant and feasible measures that organisations can realistically implement. At the same time we aim at broadening the support and feasibility of digital security for all companies in Europe.

Table of contents

1. Executive summary

A certification scheme is "a system of rules and procedures for managing and carrying out certification of products, realization processes, services, management systems and the qualification of persons. A certification scheme describes the subject of the assessment in question and what requirements apply."

Based on this definition, the scheme for the application of the NIS2 EU Directive (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022L2555) for the interpretation of the NIS2 Supply Chain standard by the Quality Innovation Foundation is formulated here. These standard lays down the duty of care, duty of notification and supervision of the way in which the European Union interprets threats in the field of cybersecurity.

In the development of the standard, we explicitly looked at related standards such as ISO 27001 and similar standards, best practices and frameworks in Europe. With the knowledge of existing standards in mind, we developed a vision together with specialists and experts and applied it to the guideline. From there, we developed the standard, translated it into measures and formulated the corresponding assessment criteria. This includes both concrete control measures and measures at system and organisational level. We then tested the standard with lawyers and recognized cybersecurity specialists. By creating 3 levels, SC10, SC20 and SC30, we have made the standard suitable for various target groups such as smaller (SME) companies and medium-sized and large organisations. Especially for all those who do not have their own expertise and capacity in the complex field of cybersecurity. Where we speak of standard in this document, you can therefore read the three NIS2 SC standards.

The NIS2 Supply Chain Compliance and Certification Scheme is aimed at making clear what all parties involved can expect from the operation of the scheme, especially when it comes to the practical application of the scheme. At the same time, the scheme has been kept more global than existing schemes, such as for the ISO/IEC standards for management systems and information security.

2. Introduction

The NIS2 Supply Chain Compliance and Certification Scheme has also been developed to provide companies and organisations, large and small, with recognition for measures taken in the field of digital security, appropriate to the size and complexity of their organisations and the importance of their role in the supply chain.

The development was done at the request of, by and with industry and professional organisations. The standard is intended for their members. These members, companies of all sizes, are experiencing a growing regulatory burden from various laws, which is reason enough to choose a standard with an appropriate character.

For the NIS2 Supply Chain Compliance and Certification Scheme, the same system was used as the European Cybersecurity Agency ENISA does for the creation of ICT products and services. According to the ENISA website: "The EU cybersecurity certification framework lays down the procedure for the creation of EU-cybersecurity certification schemes covering ICT products, services, and processes. Each scheme will specify one or more levels of assurance (Basic, Substantial, or High) based on the level of risk." We will therefore apply the principle of 3 levels (Basic, Substantial, and High) to the NIS2 Supply Chain.

3. Version control

The Quality Innovation Foundation ensures careful version management of all documents and data in relation to the requirements used for the NIS2 Supply Chain Compliance and Certification Scheme. This draft version builds on the 'NIS2 Supply Chain Compliance and Certification Scheme' of 5 October 2023, with the Basic v2, Substantial and High standard lists of the 15 February 2024 versions as an appendix. The status as of September 9, 2024, is draft number 2.9. The official version 3.0 is from October 16, 2024.

The following versions have been adopted:

Table 3.1 Standard	Version	Date
NIS2 Supply Chain	V 1.0	31-10-2023
NIS2 Supply Chain	V 2.0	15-02-2024
NIS2 Supply Chain	V. 3.0	16-10-2024
NIS2 Supply Chain	V. 3.1	8-4-2025
NIS2 Supply Chain	V. 3.2	1-1-2026

In version 3.2 of 01-01-2026, various points for improvement have been brought together in the prelude to version 4.0.

Companies and institutions work across borders, with contacts and exchanges all over the European Union. For this reason, the standard and associated measures have been formulated in such a way that they are applicable everywhere in all Member States, including for the direct suppliers of NIS2 entities in the Member States. The standard will be available in several languages, starting with English and Dutch. The English version is leading. This is done as far as possible in line with the points of attention formulated by ENISA and other European institutions.

The realisation of this scheme and their elements will take place in several steps. Both the working method, the audits themselves and the supporting processes are tested by qualified persons. Even after this test phase, quality is monitored in the context of the feedback steps as described in chapter 16.

Table 3.2	Testing (t)	Baseline measurement	Test from
10.1	Developing process diagrams	Q1-2024	Q3-2024
10.1.1	Trial audit(s) SC10 Foundation for Quality Innovation	Q2-2024	Q4-2024
10.1.2	Digital data flow testing and process steps	Q2-2024	Q43-2024
10.2.1	Trial audit(s) SC20 Quality Innovation Foundation	Q4-2024	Q1-2025
10.1.2	Digital data flow testing and process steps	Q2-2025	Q1-2025
10.2.3	Trial audit(s) SC30 Quality Innovation Foundation	Q2-2025	Q2-2025

4. Purpose of the NIS2 Supply Chain Compliance and Certification Scheme

The NIS2 Supply Chain Compliance and Certification Scheme has been developed to support organisations across Europe in the implementation of the NIS2 directive. The NIS2 Supply Chain Compliance and Certification Scheme has been developed to support organisations across Europe in the implementation of the NIS2 Directive. The NIS2 aims to take cybersecurity in the European Union to a higher common level by strengthening the digital resilience of 'essential and important entities' in the Member States, as they play a critical role in this. Many more organisations are vulnerable to digital threats through the chain.

This scheme focuses primarily on the direct suppliers in the supply chain of these entities, SMEs. The critical entities are asked to identify their direct suppliers and service providers and to limit their risks in the chain.

In addition, the scheme may also be relevant for consultancy firms, providers of Governance, Risk & Compliance (GRC) software and audit firms. The scheme provides a standardised tool that enables them to effectively and efficiently meet the requirements of the NIS2 Directive.

The NIS2 Supply Chain Compliance and Certification Scheme can give participants, industry organisations and the public the confidence that the standard leads to a higher level of digital security at the participating organisations. The SC10, SC20 and SC30 standards form a whole that considers the elements of the European directive at both system level and the level of concrete measures. Together, the three levels within the scheme indicate a development path towards a step-by-step increase in cyber resilience in line with the NIS2 guideline and the duty of care for suppliers can be met. The participating companies themselves determine the level that suits their needs, sector and risks.

This means that not only is a standard provided for a certain period, but that reference is also made to activities that can be carried out in the period up to the next assessment. This gives the standard a dynamic character, appropriate to increasing threats. NIS2 Supply Chain is therefore a dynamic standard that grows every year and in which companies must arrange one or more new things every year. The aim is to stimulate continuous improvement and innovation within companies through annual additions to the standard. These include:

- Findings and stimulating suggestions during the audit and in the report that can give direction to next steps.
- References to resources that can help with next steps, including formats and other resources.
- Each of the three levels remains essentially unchanged and forms the basis for the audit criteria. However, one or more new requirements or points for improvement can be added to the standard every year, to strengthen the supply chain. These will be included in a subsequent audit.
- Changes in the practice of the tests in the form of internal or external audits if there are new developments, such as through Artificial Intelligence, that may affect cyber resilience.

5. Governance

The governance of NIS2 Supply Chain Compliance and Certification Scheme involves various actors, leading to different activities:

The NIS Quality Mark Compliance and Certification Scheme was developed on behalf of the Quality Innovation Foundation. The standard has been developed and established at a substantive level by the Standards Committee, with input from teams of experts. The audits are carried out on this basis, supported by the audit organisation.

The following **roles** can be distinguished:

- **The Quality Innovation Foundation ('Stichting Kwaliteitsinnovatie'):** Commissioning body responsible for initiating and overseeing the development of the NIS2 Supply Chain and as such also Scheme Owner.
- **Standards Committee:** Responsible for formulating the standard and compliance, in this case the NIS2 Supply Chain Compliance and Certification Scheme. This consists of representatives of industry and professional organisations.
- **Round Table of Auditors:** Specialists with demonstrable highly qualified knowledge and experience in auditing cybersecurity measures. They contribute to the content and quality of NIS2 Supply Chain standards, NIS Quality Mark Compliance and Certification Scheme, The NIS2 Supply Chain Audit Guide, the digital audit tool and pay specific attention to the quality of the audits.
- **Expert teams:** teams that are jointly responsible for creating the standard. A communication team, a team of lawyers, a team of standards specialists and a team of technical specialists and a team of cybersecurity consultants.
- **Auditee:** The organisation being audited.
- **Auditor:** Performer of the audit and the associated interview with the auditee based on a service agreement and the desired approach. Responsible for the assessment based on the standard of the auditee. Based on a license agreement with the Quality Innovation Foundation, the auditor obtains the right to carry out audits regarding this NIS2 standard.
- **Auditors:** Individuals or audit organisations that meet the qualifications and are recognized by the Quality Innovation Foundation.
- **Audit organisation:** Supporting organisation for the planning and execution of audits.
- **Implementing organisation:** Supporting organisation for the activities of the Quality Innovation Foundation, including the establishment and maintenance of the registers
- **Register:** Information about all organisations that have obtained their certificate or intend to do so through a pre-registration. In addition, the register of qualified auditors and their organisations.

- **Complaints Committee:** An independent part of the Quality Innovation Foundation that provides an independent opinion on complaints if requested by an auditor or auditee.
- **Sampling:** an unannounced review of completed audits to ensure quality and consistency.

The following definitions **apply to the various terms and activities**:

- **Information security:** Protecting the availability, integrity and confidentiality of the information for which the auditee is (partly) responsible.
- **Cybersecurity:** the part of information security that focuses on protecting information, systems, networks and applications against digital attacks.
- **Audit report:** the auditor's report/report, to be kept for quality purposes for 3 years and 3 months.
- **Control measure:** A control measure can be any process, policy, facility, working method or other measure that changes the risk.
- **Evidence:** any documents or systems that the auditee shows or shares with the auditor.
- **Operational Technology (OT):** Collective term for various systems that are used to manage operational processes in the physical world.
- **User:** Interested party with access to one or more information systems of the organisation (for example: employees, customers, suppliers).
- **Threat:** Potential cause of an unwanted incident that could result in damage to a system or an organisation.
- **Vulnerability:** Weak point of an asset or control measure that one or more threats can use.
- **Incident:** Separate or series of events that are highly likely to compromise business operations and compromise information security.
- **Outsourcing:** Entering into an agreement in which an external party carries out part of an organisation's process. The organisation remains jointly responsible for the outsourced process, including the control measures.

The following **sources and documents** support the audits:

Certification and compliance scheme: this document

Audit Guidelines: document containing guidance for the content audit during the audit

Audit Guide: document as step-by-step guide for the execution of the audit and the use of the tool

Audit Tool: excel document that is the base for the findings of the audit and its report

Audit website: www.nis2supplychain.eu where the auditor can find news, documents, training dates and more

6. Scope

6.1 Who can use the tool?

The NIS2 Supply Chain Compliance and Certification Scheme is a tool to comply with the NIS2 directive.

All organisations that wish to use this tool are free to do so. All organisations, from large to small, SMEs, large institutions, self-employed persons, multinationals, foundations, associations, cooperatives, federations and industry and professional organisations, etc., regardless of the sector. The report follows the description given by the auditee in pre-registration.

6.2 Suitable for SMEs

This compliance and certification scheme covers all organisations that fall under the scope of the NIS2 Directive and its national translations into legislation, in particular Article 7 of the Cybersecurity Act and Article 23 of the NIS2 Directive. Within this, explicit attention is paid to the target group of SMEs and smaller institutions.

In addition to the assessment, activating the (SME) companies involved is also essential to give this standard added value for all involved. The NIS2 Supply Chain Compliance and Certification Scheme was developed with explicit regard to the requirement to "Ensure that SMEs are not required to follow costly and complex testing regimes" (5.4.4) and to require "simple and cost-effective methods of verifying compliance". This CEN-CENELEC Guideline 17 will become part of the test of the scheme, with a 0 measurement for the full start and a 1 measurement.

There are three levels at which the standard can be used:

- SC10 at basic level
- SC20 at a substantial level
- SC30 at high level

The choice of standard is based on the risk level and the expectations of the chain partners. There is no mandatory order in achieving the standards. Organisations may start at any level (SC10, SC20, SC30 depending on their risk profile and the expectations of their supply chain partners. For example, small-scale companies and institutions with a limited risk will benefit from doing or starting the SC10. If there are higher expectations, the SC20 or SC30 can also be chosen immediately.

7. Core of the NIS2: risk analysis, risk management, reporting obligation, incident response and Article 21.

This NIS2 Supply Chain Compliance and Certification Scheme is based on the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on "measures for a high common level of cybersecurity across the Union." This NIS2 directive has entered into force in Europe on October 17, 2024.

The NIS2 Supply Chain Compliance and Certification Scheme focuses on the confidentiality, integrity and availability of information within an organisation.

Broadly speaking, each organisation has at least:

- **Risk analysis:** the analysis of risks that may occur in the short and longer term.
- **Risk management:** Including the way in which risks are addressed and the roles and responsibilities that go with it, and the way in which these responsibilities are carried and transferred.
- **Duty to report:** Procedures for reporting to competent authorities and/or in the supply chain.
- **Incident response plan:** Every organisation must have an incident response plan, which also describes the obligation to report.
- Article 21 of the NIS2 Directive lists measures and areas of interest:

  (a) policies on risk analysis and security of information systems;

  (b) incident handling;

  (c) business continuity, such as backup management and contingency plans, and crisis management;

  (d) the security of the supply chain, including security-related aspects relating to the relationships between each entity and its direct suppliers or service providers;

  (e) security in the acquisition, development and maintenance of network and information systems, including vulnerability response and disclosure;

  (f) policies and procedures to assess the effectiveness of cybersecurity risk management measures;

  (g) basic cyber hygiene practices and cybersecurity training;

  (h) policies and procedures on the use of cryptography and, where appropriate, encryption;

  (i) security aspects of personnel, access policies and asset management;

(j) the use of multi-factor, authentication or continuous authentication solutions, secure voice, video and text communications and secure emergency communications systems within the entity, where appropriate.

The European directive contains very concrete measures that can be mapped to standards. We have done that too - the approach is 'rule-based'. NIS2 Supply Chain is mapped to article 21 of the NIS2 directive.

Organisations must therefore ensure compliance themselves. In the further elaboration of this, management must be closely involved in the NIS2.
Leadership is expected from the CEO, the C-level board. He or she must be aware of the possible risks and act accordingly.

In any case, this affects the involvement of the IT, procurement, legal and HRM departments. Together, these departments must ensure coverage of the three major risk areas: IT, suppliers and employees.

The necessary measures are named for each standard. Without pre-registration and participation in the pre-audit webinar, no audit can be conducted.

8. Standards

8.1 Features

The standards were drawn up by cybersecurity specialists, auditors and other experts on behalf of the Quality Innovation Foundation. This was then adopted by a NIS2 Standards Committee, consisting of representatives of various industry organisations. This scheme also includes a questionnaire for assessing the level of risk and a dynamic approach, as described in Chapter 4 on the purpose of the standard. The standards each have their own characteristic: SC, which stands for 'Quality Mark' and a serial number: 10, 20 and 30. A standard document has been drawn up for each standard.

Below are the general classifications of the three standards and the associated groups of measures. For each standard, a balance between the measures has been sought.

The numbering can be traced back to the standard, a part of it is selected for each Quality Mark. For each part of the standard, it is also made visible - the 'mapping' - how the standard relates to other standards.

Features and measures of NIS2 SC10 Basic:

Table 8.1	Features NIS2 SC10 Basic	
8.1.1	Principles	Minimum threshold, short-term, no specific OT and IT security measures
8.1.2	Measures:	See standard document
8.1.3	Risk assessment	Questionnaires
8.1.4.1	Number of auditors	1 per audit
8.1.4.2	Estimated net audit duration for applicant/auditee	See table
8.1.4.3	Estimated audit duration for auditor (if pass)	See Table 8.5

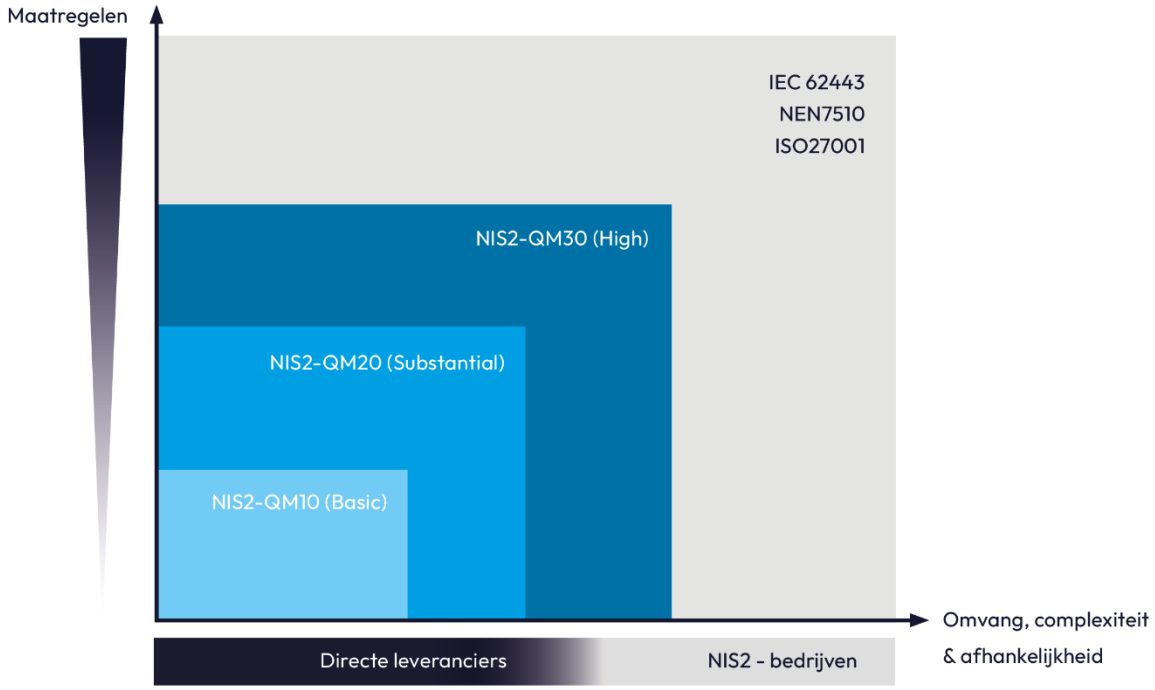
Features and measures of NIS2 SC20 Substantial:

Table 8.2	Features NIS2 SC20 Substantial	
8.2.1	Principles	Logical walk-through on Basic, strengthening P-D-C-A, technological OT and IT security measures
8.2.2	Measures	See standard document
8.2.3	Risk assessment	Questionnaires + report on possible improvements
8.2.4.1	Number of auditors	1-2
8.2.4.2	Estimated audit duration for applicant/auditee	See table
8.2.4.3	Estimated audit duration for auditor (if pass)	See Table 8.5

Features and Measures of NIS2 SC30 High:

Table 8.3	Features NIS2 SC30 High	
8.3.1	Principles	Logical run-through at Substantial, strengthening P-D-C-A, extensive attention to OT and IT security measures
8.3.2	Measures	See Chapter 22
8.3.3	Risk assessment	Questionnaires + report of possible improvements
8.3.4.1	Number of auditors	1-2
8.3.4.2	Estimated audit duration for applicant/ Auditee	See Table 8.3.2 or Audit Guide
8.3.4.3	Estimated audit duration for auditor	See Table 8.5

8.2 A ladder for growth



The European Commission has named the supply chain in its European NIS2 directive. This implies challenges at many levels in business and society as a whole. A much larger number of companies and organisations are affected by this. Not only the often somewhat larger NIS2 organisations and companies, but also the smaller companies and SMEs (suppliers). ENISA works with adapted processing at multiple levels in the context of other cybersecurity directives. The basic assumption is that SMEs cannot immediately meet the same compliance standards as large multinationals.

Standards have been formulated at three levels. These levels form a ladder for companies that fall under the scope. This allows them to dynamically develop to the higher safety levels: from Basic via Substantial towards High. If desired, organisations can then connect to ISO27001/NEN7510 and other comparable standards.

8.3 Duration and duration of assessment

8.3.1 Duration

The audit has a 3-year repeat cycle. The 3 levels also come with different assessment levels.

Assessment	Basis	Substantial	High
Standard	NIS2 SC10	NIS2 SC20	NIS2 SC30
Type of review	Certification	Certification	Certification
Assessment method	Certification based on validated self-assessment and/or remote measures	Self-assessment certification with on-site assessment	Certification audit
Review by	1 auditor with defined qualifications*	1-2 auditors with defined qualifications*	1-2 auditors accredited audit firm
Accreditation standard	ISO/TEC 17029 and/or permission from the Quality Innovation Foundation	ISO/TEC 17029 and/or ISO/TEC 17021 and/or permission from the Quality Innovation Foundation	ISO/TEC 17021-1 and/or permission from the Quality Innovation Foundation.
Proof of compliance	Completed audit or analysis with positive result	Completed audit with positive result	Completed audit with positive result

- A review auditor is assigned to each auditor to ensure quality and consistency. More auditors can also be deployed in larger companies (see Chapter 10).

8.3.2 Indication table duration per audit

Table A: Basic number of audit hours			
FTE	**SC10**	**SC20**	**SC30**
SME ≤ 10	4	8	20
SMEs 11 - 25	8	12	24
SMEs 26 - 100	16	20	36
SME 100 - 250	24	32	40
SME > 250	*on request*	*on request*	*on request*
NIS2 org <25	12	16	28
NIS2 org <=100	20	24	40
NIS2 org ≤ 500	32	40	48
NIS2 org > 500	*on request*	*on request*	*on request*

Table B: additional audit hours for locations / legal entities			
B.1 IT is not centrally controlled			
Locations / legal entities 2 < 5	4	8	12
Locations / legal entities 6 - 10	8	16	24
Locations / legal entities 11 - 25	16	32	48
Locations / legal entities 26 - 100	*on request*	*on request*	*on request*
Locations / legal entities > 100	*on request*	*on request*	*on request*
B.2 IT is centrally arranged			
Locations / legal entities 2 < 5	2	4	6
Locations / legal entities 6 - 10	4	8	12
Locations / legal entities 11 - 25	8	16	24
Locations / legal entities 26 - 100	*on request*	*on request*	*on request*
Locations / legal entities > 100	*on request*	*on request*	*on request*

Table C: Discount to avoid double testing			
Is the auditee ISO27001 or NEN7510 certified?	-60%	-60%	-60%

How does the above work?
Take the value from Table A.
Add to that the value of Table B1 or B2.
The result is the total number of audit hours.

Online and or on location?
Audits are entirely online at SC10.
With SC20, audits are online. In the event of more than 24 hours of audit time, at least one half-day on location applies.
With SC30, audits are online and on-site. In the event of more than 24 hours of audit time, a minimum of one full day on location applies.

Locations / legal entities:
Take the highest of the two. Only count the legal entities that you want to have certified.

Audit Time:
Audit time is always at least 4 hours
Audit time is the sum of the above tables. The audit time includes preparation and reporting.

Based on the above, estimates can be made of the required audit time. A distinction is made between the size of the participating companies and institutions, the question of whether it concerns a company and institution that is obliged to participate in the NIS2 directive and the number of establishments.

If a company or institution already has a different cybersecurity standard, this can affect the time to be spent. See Mapping 9.3.

For an explanation of the exact times and content of the audits, including the certificate issuing process, see the Audit Manual and Guidelines. These documents, together with a digital audit tool, is made available to audit organisations that have been appointed as auditors on behalf of the Quality Innovation Foundation.

If the audit fails on a maximum of two components, the auditee will be given the opportunity to rectify these specific points within a period of up to three months.

For each unsatisfactory part, two extra hours will be charged for the extra assessment. However, the certificate will be issued immediately as soon as the Foundation adopts the auditor's positive advice, provided that the measures in question have been demonstrably implemented within the set period. If no proof of recovery is provided within this period, the certification will be withdrawn.

9. Relationship with other standards and mapping

9.1 Relationship with other standards

The NIS2 Supply Chain Compliance and Certification Scheme is based on the Network and Information Security Directive 2 (NIS2) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022L2555).

The implementation looked at common security choices and recommendations by cybersecurity specialists. These measures are widespread in today's cybersecurity world and are reflected in most common systems, norms, schemes and standards.

Within this scheme, our own measures have been made based on input from many experts and representatives of sectors, considering measures that add the most safety and the least burden in combination with the obligations as described in the NIS2.

9.2 Mapping with other schedules, standards and frameworks

Nobody works in a vacuum. All companies have already taken measures for their cybersecurity, consciously or unconsciously, through standards or together with their IT company. So, no one starts from scratch. A mapping has been made on the most common standards. This mapping is incorporated into each of the NIS2 SC standards.

Table 9.2	Mapping	Release date:
Table 9.2.1	Mapping SC - NEN-ISO 27001	
Table 9.2.2	NIS2 SC10 Basic	15-08-2024
Table 9.2.2	NIS2 SC 20 Substantial	15-08-2024
Table 9.2.3	NIS2 SC30 High	15-08-2024

9.3 Avoiding exemption and duplication of work through Mapping

If a company or institution wants to be eligible for the NIS2 Supply Chain and another standard has already been achieved, they do not have to redo the components that have already been demonstrably achieved in the other standard. Mapping can be used to determine which parts are comparable to each other. Measures that have already been taken do not have to be redone and are exempt from the obligation to audit, provided that the standard has been assessed within 2 years before date. For further details, see the Audit Work Guide.

10. Qualifications for assessment

10.1 Qualifications

A distinction is made between the expertise requirements for auditors for auditing the Basic, Substantial and High qualifications. The performance of audits is entrusted to audit organisations recognized by the Quality Innovation Foundation that have the task of deploying auditors and monitoring the qualifications of the auditors to be deployed. A distinction is made between:

- Audit organisations that are qualified to act as auditors on an individual basis and demonstrably have the necessary knowledge of standards and audit techniques. After training, they are recognized as auditors by the Quality Innovation Foundation and are entitled to audit and/or diagnose the SC10 and partly the SC20 (the companies and organisations that do not fall directly under the NIS2).
- Audit organisations that are accredited certification bodies (CBs) and as such employ audit-qualified staff, including adequate support. The qualifications appear to be based on the (see table of standards). These licensees are entitled to audit all NIS2 SC standards.

Only auditors, audit organisations and CBs that are recognized by the Quality Innovation Foundation can conduct NIS2 SC audits independently and apply for and issue a NIS2 Certificate for their auditee. Recognition can be applied for through the Quality Innovation Foundation.

Supporting documents can be found on the Auditors page of the NIS2 Supply Chain website:

Audit Instruction: step by step overview of necessary actions for the use of the Audit Tool and a successful and complete audit.

Audit Tool: digital audit tool available to Audit Organisations and their qualified auditors to report on the audit.

Audit Guidelines: detailed overview of the content of each element of the standards with possible questions and checks for the auditor to use while performing an audit.

11. Training Auditors

The NIS2 SC standards attach great importance to well-trained employees. Training in cyber risks is a regular part of the companies themselves, also for the board members. The same applies to the auditors.

The training is half a day and focuses mainly on the audit interview. Knowledge about the NIS2 standards and method of assessment and technical knowledge about cybersecurity must already be present.

Topics that strongly determine the competence of the auditor and are discussed in the training are:

- Knowledge of standards, application of technical knowledge and assessment of risks
- The process of the audit, including Audit Tool and accompanying documents
- Conversation
- Promotion
- Reporting

For the licensees (certifying bodies/scheme owners), the requirements are laid down in an agreement. These also include the qualifications.

This is further elaborated in the document 'Audit guidelines' to be found at a special page on the website and supported by an Audit tool with instructions.

12. Applying and applying for certification

Companies and organisations that want to obtain the NIS2 Supply Chain Compliance and Certification Scheme must complete the following steps:

- Do the mandatory pre-registration via the NIS2 SC website.
- Go through steps and measures as described in the standard.
- If necessary, call in external support. There are many parties who have knowledge of the matter and can provide support.
- Participate in the mandatory pre-audit webinar and make additions and/or corrections where necessary.
- Select an audit organisation.
- Conclude an agreement with the audit institution of your choice.
- The audit body performs the test or diagnosis and assesses whether your organisation meets the requirements on the basis of documented information, interviews and observations.
- Carry out repairs within 3 months if there is reason to do so.
- The certificate is issued if the certifying body judges that your organisation meets the requirements of the NIS2 SC.
- The certificate is valid for three years.

12.1 Applying for certification via pre-registration

Upon registration, the company or institution is registered by the Quality Innovation Foundation. This can be done directly through a so-called 'pre-registration'. The confirmation provides further information about the process. The application will be definitively processed if the application contains all the necessary elements.

12.2 Application for certification

The application for certification to the Quality Innovation Foundation contains the following information:

- Organisation name, full address, contact name, contact details and the organisation's company number.
- The registration number (obtained at the time of pre-registration)
- The number of employees of the organisation.
- Date of the review.
- The version of the NIS2 Supply Chain Compliance and Certification Scheme for which one wishes to be certified.
- An advice or diagnosis from the auditor/audit organisation to the Quality Innovation Foundation that auditee meets the requirements of the NIS2 Supply Chain as laid down in the NIS2 Supply Chain Compliance and Certification Scheme.

12.3 Elements of the audit

In every audit, the following elements in the process are recognizable:

Table 12.2.1	Process: Audit Execution	From auditor's perspective:
1	Research phase: evaluation of evidence provided	Reviewing evidence.
2	Conducting an audit interview	Risk-based discussion of possible shortcomings and risks. Tests per standard element based on the chosen Quality Mark.
3	Rounding, feedback and stimulation	Finalize conversation, feedback, stimulate where necessary.
4	Reporting	Submitting advice or diagnosis to the Quality Innovation Foundation for application and assessment of certification
5.	Issuing certification or reassessment (review)	Evaluate

12.4 Assessment of the audit

The initial assessment is made on the basis of all the evidence provided. After that, an on-site or remote assessment will take place in which a complete picture can be formed of the extent to which an organisation meets the minimum requirements to obtain certification through questions and an interview.

A full assessment is carried out every three years. Each review has a score.

Each standard has mandatory measures that must be in order in the audit and other measures. An optimal audit has a balance between assessing measures and discussing findings in a stimulating way, and providing such a lower limit can help auditors make their choice. The mandatory measures are published in the Work Guide for the audit.

The score for the compulsory components must be at least a pass (6 or higher out of 10) in order to receive a certification. Of all other components, individual components may score an unsatisfactory score, but the total of all measures must have an average of 6.0 out of 10 or higher. Details can be found in the Audit Work Guide.

12.5 Reporting of the audit

The reporting of an audit includes:

- Determination of the identity of the applicant/auditee and date(s) of assessment in combination with the registration number obtained.
- Description of assessed measures and the assessment of these measures in the form of a certification advice.
- Documents and people/functions involved.
- Results of risk analysis and expectation about approach to outcomes by auditee.
- The results and evidence of the audited or diagnosed parts of the standard that apply and are discussed in the interview and lead to a decision about compliance or non-compliance. These must be kept for at least three years and three months for quality purposes.
- Statements about compliance or non-compliance and the associated period to make improvements, while considering the corresponding period of no more than 3 months.
- Any indications for stimulation in the reporting in relation to the audit result.
- Other matters and/or comments that are relevant to an evaluation.
- The report is intended exclusively for the auditor and the audit laboratory and is only accessible to persons responsible for quality assessment in the manner described in chapter 17 on quality assurance.

13. Dynamic nature of the standard

13.1 Stimulating further growth

As an extension of the audit, incentives can be proposed on all essential aspects of the audit: risk analysis, standard and in the context of the opinion. This is in line with the stimulating objective of the approach: after the Basic level, there is still a way to go on the ladder, and we want to support companies and organisations in this. The Quality Innovation Foundation compiles a list of these measures, including a brief description of possible relevance. This can be referred to in the audit report.

These incentives from the list are in line with the results of the audit, point in the direction of measures that are suitable for successor standards such as the SC20 and SC30 and do not include any advice or obligation.

In addition, every certified company or institution receives activities every year that support them to move to the next step on the audit ladder in terms of cybersecurity.

Table 13.1	Process: incentives
13.1.1	List of incentives
13.1.2	During audit: selection of incentives
13.1.3	Refer to support and training
13.1.4	Results to follow
13.1.5	Share with a digital platform

13.2 Duration of operation of the standard

A certificate for compliance with the standards of Q10, SC20 and SC30 is issued for the duration of 3 years. During that time, the standard must be maintained. This is all the more true since developments in the field of cyber resilience are moving very fast and developments such as AI (Artificial Intelligence) are being added and have an impact. For this reason, a validity period of longer than 3 years is not appropriate. In addition, we expect that this dynamic requires regular maintenance of the standard and its application. Companies should therefore consider that interim elements can be added for each standard and certainly for the SC30 there can be several.

Companies are asked to take these adjustments into account, also with a view to possible recertification. For the SC30, there may be an annual review from 2026 if developments give cause to do so.

14. Digital security requirements

ICT platforms and programs that commercially exploit the NIS2 Supply Chain must be highly secure. They must be checked for safety via pen tests and must provide proof of this. Specific security agreements will be made with each party that will carry out and/or audit the NIS2 Supply Chain. In addition, agreements are recorded in the 'Work Guide for the audit'.

We will mainly look at and pay attention to the following technical and organisational matters when we agree on a collaboration with a GRC and/or audit party. In those cases, the following have been considered and/or the following has been taken into account:

- Secure data exchange with auditee.
- Secure login (MFA or similar).
- Access to audit data is reserved exclusively for the auditor.
- Demonstrate that the application is demonstrably protected, for example by submitting a PEN test result.
- Demonstrably having appropriate cybersecurity certification or being exempted from it on the basis of demonstrable experience.

15. Legal frameworks

The application and testing of the scheme must consider the use in different domains and the associated legal frameworks:

- Assessment of the governance of the (judgment) regarding the audits for the Quality Innovation Foundation.
- The latest version of the NIS2 Directive in the English language is the current version for the Member States of the European Union.
  In the member states of the European Union, the NIS2 directive can be translated into their own laws and regulations. It is up to the companies and institutions involved to follow these national focuses and to the licensee(s) to apply them additionally during the audit. The NIS2 Supply Chain Compliance and certification scheme should therefore only be seen as a generic tool and not as "the translation of the NIS2 legislation" in a member state.
- Relevant European regulations, in particular NIS2 and related regulations under development in the field of privacy and artificial intelligence, are also expressly part of this.
- Industry-specific regulations of the participating companies, insofar as they force deviating use of the standards used within this scheme, are also part of this.

16. Use of the standard and logo by certificate holders

	Use of quality mark		
16.1	Description of the quality mark and logo		Dark blue shield on white background, with square with finch sign in it. Next to it is the name 'NIS2' and below that 'Quality Mark'.
16.2	Terms of use of third-party quality mark		Use of the quality mark and the associated expressions only after prior permission by the Stichting Kwaliteitsinnovatie, Noordwijk, the Netherlands. Requests should be sent to the Quality Innovation Foundation by e-mail: info@nis2qualitymark.eu.
16.3	Copyrights and Licenses		© All intellectual property rights, including copyrights, trademarks and design rights in and to this cybersecurity standard are reserved. You may not copy, modify, or otherwise use any part of this document without prior permission. This document is dynamic in nature. This is version 3.1 from April 8, 2025. Consult the most recent version on www.nis2qualitymark.eu.

17. Judgments on the functioning of the system

Judgments on the operation of the system set up based on this scheme are made at the level of:

- Evaluations per audit
- Complaints and objections
- Sample evaluation

17.1 Evaluations per audit

Digital evaluations are carried out based on the 'evaluation criteria NIS2 SC audit' and 'evaluation criteria NIS2 SC auditor' among participants and auditors, with opportunities for direct feedback and suggestions. Reporting, analysis, recommendations and implementation of the improvement actions are carried out by the Quality Innovation Foundation.

17.2 Complaints and objections

A complaints and disputes committee is linked to the standard. Members of these come from participating industry associations, among others. This committee is still being set up and is independent of any judgment by the Quality Innovation Foundation.

Complaints can be addressed to and collected in an accessible way by the Quality Innovation Foundation. The Quality Innovation Foundation strives for a response period of one week and will take measures quickly in the event of a well-founded complaint.

The Quality Innovation Foundation analyses any complaints in an annual quality report and makes them part of the evaluation of the system and brings them to the attention of the foundation, together with recommendations.

17.3 Random Evaluation

Random evaluation is aimed at a broader assessment of the added value of the approach. It shall include at least:

- Evaluation at the level of participants.
- Evaluation at the level of auditors.
- Evaluation at the level of licensees (according to the nature of activities and adaptation to the NIS2 approach).
- Evaluation at context level (change of standards, determination of the balance between stimulation and control and related developments such as in the field of privacy, use of AI and the like).

18. Exceptions, points of interest, volume, future developments and growth.

Defined qualifications

Chapter 8.3 states that audits can be carried out by parties with defined qualifications. We assume that it will be necessary to distinguish between accredited cybersecurity auditors, ICT auditors, seniors, mediors and juniors in every possible combination. The available number of auditors must not become a bottleneck for the implementation of NIS2 in Europe. Only auditors and audit parties that are recognized by the Quality Innovation Foundation can perform NIS2 SC audit.

Exceptions

The Quality Innovation Foundation expressly reserves the right to grant deviations if situations give cause to do so.

Self-assessments

There is the possibility for companies and organisations to do a self-evaluation. This could create the need to derive a temporary status from it. For example, in the case of waiting lists for audits. Only in that case can companies and organisations apply for temporary status through a pre-registration. The Quality Innovation Foundation expressly reserves the right to grant deviations if situations give cause to do so.

Points of attention

Rapid developments in the field of cybersecurity, such as the use of AI by criminals, the developments of Quantum computing and the emergence of new faster ways in which cyber incidents develop, require continuous attention from the Quality Innovation Foundation. For this reason, each standard is given a dynamic character, as described in Chapter 13. Collaboration is essential and we call on all market and knowledge parties to share relevant information with us.

19. Confidentiality and data protection

All parties named in the schedule are bound by confidentiality about customers and activities and sign a statement to this effect when entering into a short-term or long-term agreement or commencement of employment.

The Quality Innovation Foundation falls under the legal rules imposed by the General Data Protection Regulation (GDPR) on the processing of personal data. The organisation meets the requirements set by the GDPR.

All standard texts can be found on https://nis2qualitymark.eu/normpage/

20. Copyright and Disclaimer

Although the measures included in the NIS2 Supply Chain and related overview of measures have been developed by experts and compiled with the greatest possible care, no guarantees are given with regard to the correctness, completeness, reliability, suitability, or availability of the NIS2 Supply Chain and the information, products, services, or related graphics contained therein. The use of the NIS2 Supply Chain and related overview of measures are entirely at the risk of the user. Any liability for damage, direct or indirect, arising from or in any way related to the use of the NIS2 Supply Chain and related overview of measures is excluded.

The NIS2 Supply Chain mapping overview may include references to other standards, including ISO 27001:2022 and NEN 7510, for informational purposes only and to identify possible coherence or interfaces. These references do not imply association or endorsement of the content of the other standards. The NIS2 Supply Chain 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 the respective rightful owners of those standards.

21. National implementation of NIS2

Within the European Union, the NIS2 Directive was drawn up to strengthen digital resilience. However, it is important to understand that a directive is not a regulation. Where a regulation is directly applicable in all Member States, a directive sets objectives that must be transposed into national law by each country individually. This gives Member States the only room to decide for themselves how to implement the directive.

This freedom leads to differences between countries. For example, Member States choose which body is responsible for monitoring compliance. The interpretation of sanctions is also determined nationally: although the directive sets an upper limit on fines, countries can decide for themselves how strict or flexible they enforce, as long as the sanctions are effective, dissuasive and proportionate. In addition, countries may impose additional requirements on companies, on top of the minimum requirements of the directive.

Another important point is that Member States have room to make their own choices in the sector classification. The directive contains a European list of essential and important entities, but countries may add sectors or types of companies. Finally, the way in which companies demonstrate their compliance – for example through audits or certificates – is not defined by the EU, so it can vary from country to country.

For companies that operate across borders, this national freedom means an increase in complexity.

We strive to keep the NIS2SC as similar as possible in all countries. At the same time, this is sometimes not possible or desirable.

After the NIS2 has been implemented in all countries, we will start mapping the deviations per country. Until then, we will only include indications as far as they are known to us.

We invite everyone to report deviations that already apply in the various countries to us via the website nis2qualitymark.eu

Indications of deviations in Europe:

Netherlands:

The current draft of the Cybersecurity Act (Cbw), [1]in particular Article 7, the Cybersecurity Decree (Cbb)[2] and the Critical Entities Resilience Decree (Bwke).[3] Article 7 imposes on the 'critical entity' the obligation to identify its direct suppliers and service providers and to draw up policies in order to limit risks. Because it is foreseeable that this mainly concerns SMEs and that a series of obligations and responsibilities arise for them (and their suppliers), this certification scheme is a development to achieve the reduction of risks for SMEs as well and to do so in such a way that the regulatory burden remains as low as possible.

Training of directors under the Cybersecurity Act: state of affairs

[1] Cyber Security Act, consultation version 2025
[2] Cybersecurity Decision, consultation version 2025
[3] Critical Entities Resilience Decree, consultation version 2025

The draft texts of the Dutch Cybersecurity Act (Cbw) and the accompanying General Administrative Order (AMvB) state that directors of essential and important entities must have sufficient knowledge and skills to identify, understand and manage cyber risks. In doing so, the Netherlands is in line with the NIS2 directive, which states that the responsibility for cyber resilience lies with the highest management layer.

The draft General Administrative Order suggests that further requirements may be imposed on the content and form of these training courses. This includes the use of a qualified trainer, demonstrable presence during the training, and obtaining a certificate as proof. At the moment, however, there is no definitive clarity about the exact interpretation of this obligation.

The internet consultation on the General Administrative Order has now been completed, and many responses have been received, especially on this part. The Ministry of Justice and Security is currently working on the assessment of these responses. Based on this, it will be decided whether and to what extent the rules surrounding the training requirements for drivers will be adjusted.

It is important for organisations to be aware of this upcoming obligation and to think about appropriate measures, even if the final laws and regulations are still under development.

