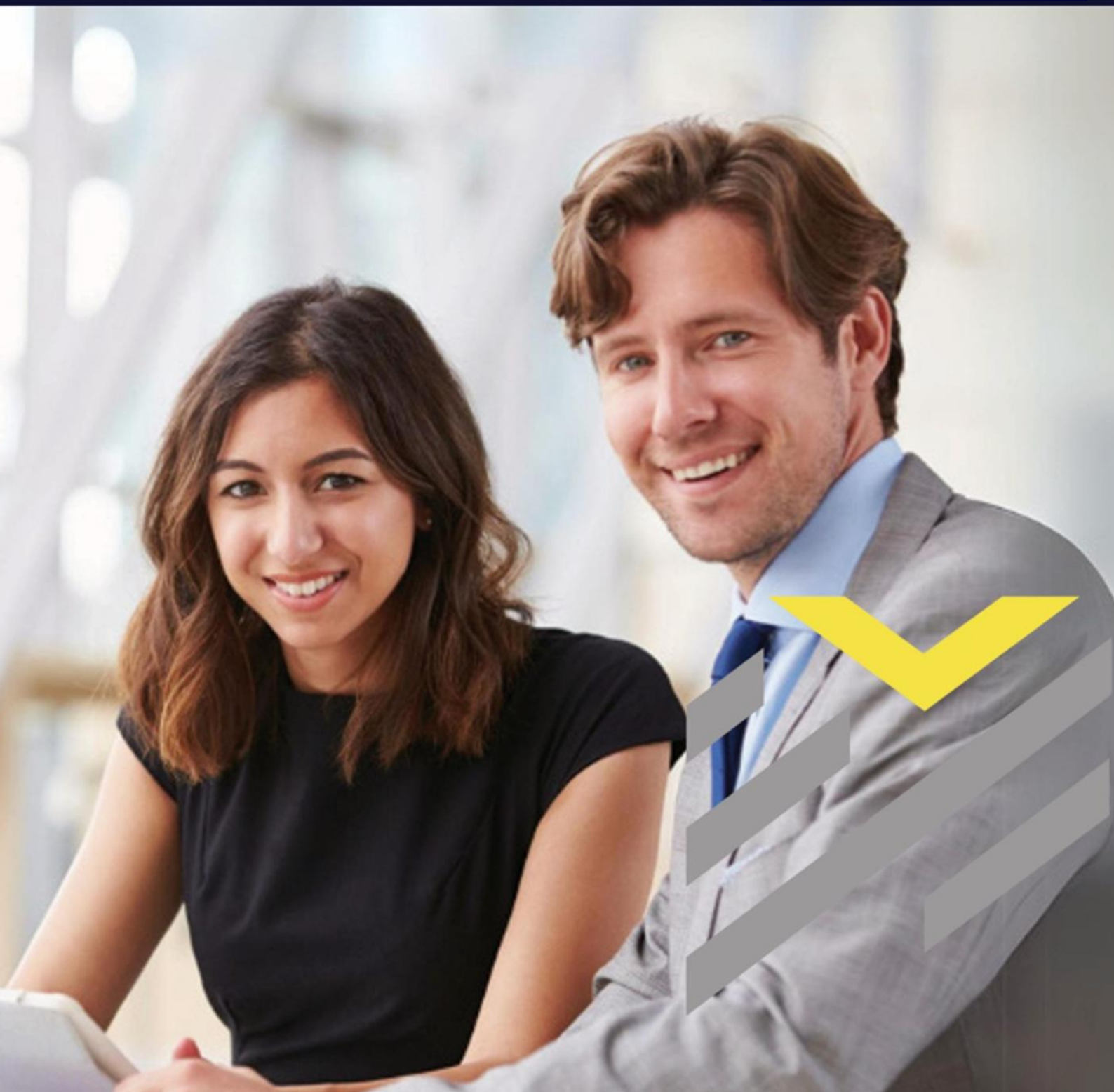
NIS2 Supply Chain Certificering

Compliance en certificeringsschema

Versie 3.2
1 januari 2026

NIS2 SUPPLY CHAIN



NIS2 Supply Chain certificering, Compliance en Certificeringsschema

Voorwoord

De NIS2 (Network and Information Security) richtlijn van de Europese Unie is een uitbreiding en vervanging van de oorspronkelijke NIS richtlijn. Het doel van NIS2 is om de digitale en operationele weerbaarheid van essentiële en belangrijke sectoren binnen de EU te versterken. De richtlijn stelt strengere beveiligingseisen en rapportageverplichtingen voor organisaties om cyberdreigingen beter te voorkomen, sneller op te merken en effectiever aan te pakken. Dit omvat alle essentiële en belangrijke NIS2 entiteiten en ook hun directe leveranciers in de toeleveringsketen.

Artikel 21.2(d) van de NIS2 richtlijn richt zich op de beveiliging van de toeleveringsketen via de directe leveranciers van producten en diensten. Dit artikel vereist dat organisaties binnen de scope van NIS2 passende maatregelen nemen om ervoor te zorgen dat hun directe leveranciers en dienstverleners ook voldoen aan de relevante beveiligingsvereisten.

Dit betekent dat deze organisaties verantwoordelijk zijn voor het waarborgen van de cybersecurity van hun toeleveringsketen (directe toeleveranciers). Ze moeten controleren en verifiëren dat leveranciers en dienstverleners adequate beveiligingsmaatregelen hebben geïmplementeerd om cyberrisico's te minimaliseren. Dit betekent dat organisaties:

- Moeten samenwerken met leveranciers om beveiligingspraktijken te verbeteren en incidentresponsprocedures te coördineren, zodat de bedrijfcontinuïteit verzekerd is bij cyberincidenten.
- Door deze maatregelen te nemen, ze de beveiliging van hun hele toeleveringsketen verbeteren en de kans op cyberincidenten verkleinen door in contracten op te nemen dat leveranciers aan specifieke beveiligingsstandaarden moeten voldoen.
- Audits en/of diagnoses en/of beoordelingen moeten (laten) uitvoeren om de naleving van beveiligingsmaatregelen door leveranciers te controleren.
- Periodieke risicobeoordelingen moeten uitvoeren van leveranciers om potentiële kwetsbaarheden en bedreigingen te identificeren.

In de toeleveringsketen zitten niet alleen grote bedrijven maar ook veel middelgrote en kleine bedrijven (mkb-bedrijven). Die hebben eigen uitdagingen als het gaat om het verhogen van hun cybersecurity:

- Mkb-bedrijven hebben vaak een beperkt budget voor cybersecuritymaatregelen, waardoor het moeilijk kan zijn om geavanceerde beveiligingstechnologieën aan te schaffen.
- Ze hebben vaak geen eigen gespecialiseerde ICT- en/of cybersecuritymedewerkers.
- Medewerkers van mkb-bedrijven zijn zich vaak minder bewust van cybersecurityrisico's en hebben mogelijk niet de nodige training ontvangen om cyberdreigingen te herkennen en erop te reageren.
- Het begrijpen en naleven van complexe regelgeving zoals NIS2 kan voor mkb-bedrijven lastig zijn, vooral zonder de hulp van juridische en compliance experts.

De Stichting Kwaliteitsinnovatie

Dit Compliance en Certificeringsschema is opgesteld door de Stichting Kwaliteitsinnovatie. Als Stichting, die werkt voor de belangen van samenwerkende branche- en beroepsorganisaties en de daar aangesloten bedrijven en beroepsbeoefenaren, streven wij naar verbetering van cybersecurity voor alle bedrijven en organisaties in Europa. Dit doen we door een breed gedragen norm in meerdere niveaus toegankelijk te maken. We kiezen voor relevante en haalbare maatregelen die binnen het bereik van organisaties liggen en tegelijkertijd het draagvlak en de haalbaarheid van digitale beveiliging voor alle bedrijven in Europa verbreden.

Het NIS2 Supply Chain Compliance- en certificeringsschema is openbaar en kan, mits ongewijzigd en met bronvermelding, worden verspreid.
Voor auditorganisaties die door de Stichting Kwaliteitsinnovatie zijn aangeduid als auditors is er een ‘Werkwijzer voor de audit’ en een digitale audittool beschikbaar.

Inhoudsopgave

1. Executive summary

Een certificeringsschema is "een stelsel van voorschriften en procedures voor het beheren en uitvoeren van certificatie van producten, realisatieprocessen, diensten, managementsystemen en de kwalificatie van personen. In een certificeringsschema staat beschreven wat het onderwerp van de betreffende beoordeling is en welke eisen er gelden."

Op basis van deze definitie wordt hier geformuleerd wat het schema is voor toepassing van de NIS2 EU-richtlijn (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022L2555) voor de interpretatie van de NIS2 Supply Chain certificering norm door de Stichting Kwaliteitsinnovatie. In deze norm zijn de zorgplicht, meldplicht en het toezicht vastgelegd op de wijze waarop de Europese Unie dreigingen op het terrein van cyberbeveiliging interpreteert.

Bij de ontwikkeling van de norm is nadrukkelijk gekeken naar verwante normen zoals ISO 27001 en vergelijkbare normen, best practices en frameworks in Europa. Met de kennis van bestaande normen in ons achterhoofd, hebben we samen met specialisten en deskundigen een visie ontwikkeld en deze toegepast op de richtlijn. Vanuit daaruit hebben wij de norm ontwikkeld, vertaald in maatregelen en hebben bijbehorende toetsingscriteria geformuleerd. Dit omvat zowel concrete beheersmaatregelen als maatregelen op systeem- en organisatieniveau. De norm hebben wij vervolgens getoetst bij juristen en erkende cybersecurityspecialisten. Door het creëren van 3 niveaus, SC10, SC20 en SC30, hebben wij de norm geschikt gemaakt voor diverse doelgroepen zoals kleinere (mkb) bedrijven en middelgrote en grote organisaties. Zeker ook voor allen die niet kunnen beschikken over eigen deskundigheid en capaciteit in het complexe vakgebied van cybersecurity. Waar wij in dit document spreken van norm kunt u dan ook lezen de drie NIS2 SC normen.

Het NIS2 Supply Chain Compliance- en certificeringsschema is erop gericht om duidelijk te maken wat alle betrokken partijen van de werking van het schema mogen verwachten, in het bijzonder als het om de praktijktoepassing van het schema gaat. Tegelijk is het schema globaler gehouden dan bestaande schema’s, zoals bijvoorbeeld voor de ISO/IEC-normen voor managementsystemen en informatiebeveiliging.

2. Introductie

Het NIS2 Supply Chain Compliance- en certificeringsschema is ook ontwikkeld om bedrijven en organisaties, groot en klein, te voorzien van een erkenning voor genomen maatregelen op het terrein van digitale veiligheid, passend bij de omvang en complexiteit van hun organisaties en het belang van hun rol in de toeleveringsketen.

De ontwikkeling is gedaan op verzoek van, door en met branche- en beroepsorganisaties. De norm is bestemd voor hun leden. Deze leden, bedrijven van klein tot groot, ervaren een groeiende regeldruk vanuit diverse wetten, reden om een norm te kiezen met een passend karakter.

Voor Het NIS2 Supply Chain Compliance- en certificeringsschema is eenzelfde systematiek gebruikt zoals het Europese Agentschap voor Cybersecurity ENISA dat doet voor de creatie van ICT-producten en -services. Volgens de 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.” Het principe van 3 levels (Basic, Substantial, and High) zullen wij dus toepassen op Het NIS2 Supply Chain certificaat.

3. Versiebeheer

De Stichting Kwaliteitsinnovatie zorgt voor zorgvuldig versiebeheer van alle documenten en data in relatie tot de gehanteerde eisen voor Het NIS2 Supply Chain certificaat Compliance en Certificeringsschema. Deze conceptversie bouwt voort op het 'NIS2 Supply Chain certificering Compliance en Certificatie Schema' van 5 oktober 2023, met als bijlage de normlijsten Basic v2, Substantial en High van de versies 15 februari 2024. De status per 9 september 2024 is concept nummer 2.9. De officiële versie 3.0 is van 16 oktober 2024.

De volgende versies zijn vastgesteld:

Tabel 3.1 Standaard	Versie	Datum
NIS2 Supply Chain certificering	V 1.0	31-10-2023
NIS2 Supply Chain certificering	V 2.0	15-02-2024
NIS2 Supply Chain certificering	V. 3.0	16-10-2024
NIS2 Supply Chain certificering	V. 3.1	8-4-2025
NIS2 Supply Chain certificering	V. 3.2	1-1-2026

In de versie 3.2 van 01-01-2026 zijn diverse verbeterpunten bij elkaar gebracht in de opmaat naar versie 4.0.

Bedrijven en instellingen werken over grenzen heen, met contacten en uitwisselingen overal in de Europese Unie. Om die reden zijn de norm en bijbehorende maatregelen zo geformuleerd dat deze in alle lidstaten overal toepasbaar zijn, ook voor de dircete toeleveranciers van NIS2 entiteiten in de lidstaten. De norm komt beschikbaar in meerdere talen, startend met Engels en Nederlands. Dit gebeurt zo ver als mogelijk is in lijn met de aandachtspunten zoals Enisa en andere Europese instellingen die formuleren.

De realisering van de onderdelen van dit schema gebeurt in een aantal stappen. Zowel de werkwijze, de audits zelf en de ondersteunende processen worden getest door gekwalificeerde personen. Ook na deze testfase wordt de kwaliteit bewaakt in het kader van de feedbackstappen zoals beschreven in hoofdstuk 16.

Tabel 3.2	Testen (t)	Nulmeting	Test vanaf
10.1	Ontwikkelen processchema's	Q1-2024	Q3-2024
10.1.1	Proefaudit(s) Stichting Kwaliteitsinnovatie SC10	Q2-2024	Q4-2024
10.1.2	Testen datastroom en processtappen digitaal	Q2-2024	Q4-2024
10.2.1	Proefaudit(s) Stichting Kwaliteitsinnovatie SC20	Q4-2024	Q4-2025
10.1.2	Testen datastroom en processtappen digitaal	Q2-2025	Q4-2025
10.2.3	Proefaudit(s) Stichting Kwaliteitsinnovatie SC30	Q3-2025	Q4-2026

In de aanloop naar het van kracht worden van de NIS2 regelgeving zijn vanaf Q4 2024 meerdere pilots gehouden bij wijze van test voor zowel de SC10, de SC20 als de SC30. Na de totstandkoming van versie 4.0 worden nieuwe testen gedaan.

4. Doel van Het NIS2 Supply Chain Compliance en Certificeringsschema

Het NIS2 Supply Chain Compliance- en certificeringsschema is ontwikkeld om organisaties in heel Europa te ondersteunen bij de implementatie van de NIS2 richtlijn. Het NIS2 Supply Chain Compliance- en certificeringsschema is ontwikkeld om organisaties in heel Europa te ondersteunen bij de implementatie van de NIS2-richtlijn. De NIS2 beoogt de cyberveiligheid in de Europese Unie naar een hoger gemeenschappelijk niveau te brengen door de digitale weerbaarheid van 'essentiële en belangrijke entiteiten' in de lidstaten te versterken, omdat zij daarin een kritieke rol spelen. Via de keten zijn er veel meer organisaties kwetsbaar voor digitale dreigingen.

Dit schema richt zich primair op de directe leveranciers in de toeleveringsketen van deze entiteiten; doorgaans mkb-bedrijven. Van de kritieke entiteiten wordt gevraagd dat zij hun directe toeleveranciers dienstverleners in beeld brengen en hun risico's in de keten te beperken.

Daarnaast kan het schema ook relevant zijn voor consultancyorganisaties, aanbieders van Governance, risk & compliance (GRC) software en auditorganisaties.. Het schema biedt een gestandaardiseerd hulpmiddel dat hen in staat stelt om effectief en efficiënt te voldoen aan de eisen van de NIS2-richtlijn.

Aan Het NIS2 Supply Chain certificaat Compliance en Certificatieschema kunnen deelnemers, brancheorganisaties en het publiek het vertrouwen ontlenen dat de norm leidt tot een hoger niveau van digitale veiligheid bij de deelnemende organisaties. De normen SC10, SC20 en SC30 vormen een geheel dat de elementen van de Europese richtlijn meeneemt op zowel systeemniveau als het niveau van de concrete maatregelen. Samen geven de drie niveaus binnen het schema een ontwikkeltraject aan richting een trapsgewijze toename van cyberweerbaarheid in lijn met de NIS2 richtlijn en kan worden voldaan aan de zorgplicht voor toeleveranciers. De deelnemende bedrijven bepalen zelf het niveau dat bij hun behoeften, sector en risico's past.

Dit betekent dat niet alleen een norm wordt verstrekt voor een bepaalde periode, maar dat ook wordt verwezen naar activiteiten die in de periode tot aan de volgende toetsing kunnen worden uitgevoerd. Zo krijgt de norm een dynamisch karakter, passend bij toenemende dreigingen. NIS2 Supply Chain certificering is daarmee een dynamische norm die jaarlijks groeit en waarbij bedrijven elk jaar één of meerdere nieuwe zaken moeten regelen. Het doel hiervan is het stimuleren van voortdurende verbetering en innovatie binnen bedrijven door jaarlijkse toevoegingen aan de norm. Daaronder vallen:

- Bevindingen en stimulerende suggesties tijdens de audit en in de rapportage die richting kunnen geven aan vervolgstappen.
- Verwijzingen naar bronnen die kunnen helpen bij volgende stappen, inclusief formats en andere hulpbronnen.

1 Network and Information Security Directive (NIS2-richtlijn (EU) 2022/2555)

- Elk van de drie niveaus blijft in de kern onveranderd en vormt de kern van de auditcriteria. Wel kan elk jaar één of meerdere nieuwe eisen of verbeterpunten worden toegevoegd aan de norm, in het bijzonder ter versterking van de supply chain. Die worden meegenomen in een volgende audit.

- Wijzigingen in de praktijk van de toetsingen in de vorm van interne of externe audits als er nieuwe ontwikkelingen zijn, zoals bijvoorbeeld via Artificial Intelligence, die van invloed kunnen zijn op de cyberweerbaarheid.

5. Governance

Bij de governance van NIS2 Supply Chain certificering Compliance en Certificeringsschema zijn verschillende actoren betrokken, leidend tot verschillende activiteiten:

Het NIS Supply Chain certificering Compliance en Certificeringsschema is ontwikkeld in opdracht van de Stichting Kwaliteitsinnovatie. De norm is op inhoudelijk niveau ontwikkeld en vastgesteld door de normcommissie, met inbreng van expertteams. Op deze basis worden de audits uitgevoerd, ondersteund door de auditorganisatie.

De volgende **rollen** kunnen daarin worden onderscheiden:

- **De Stichting Kwaliteitsinnovatie:** Opdrachtgever en eindverantwoordelijk voor het realiseren en in stand houden van erkenning door middel van een norm voor NIS2 compliance en tevens verstrekker van Het NIS2 Supply Chain certificaat Certificaat.
- **Normcommissie:** Verantwoordelijk voor het formuleren van de norm en compliance, in dit geval Het NIS2 Supply Chain certificaat Compliance en Certificeringsschema. Deze bestaat uit vertegenwoordigers van branche- en beroepsorganisaties.
- **Ronde tafel van auditoren:** Specialisten met aantoonbare hooggekwalificeerde kennis en ervaring in het auditeren van cybersecuritymaatregelen. Zij werken mee aan de inhoud en kwaliteit van NIS2 Supply Chain certificering normen, NIS Supply Chain certificering Compliance en Certificeringsschema, De NIS2 Supply Chain certificering Auditwijzer, de digitale audit tool en hebben specifieke aandacht voor de kwaliteit van de audits.
- **Expertteams:** teams die samen inhoudelijk verantwoordelijk zijn voor het creëren van de norm. Een communicatieteam, een team van juristen, een team van normspecialisten en een team van technische specialisten en een team van cybersecurityconsultants.
- **Audittee:** De organisatie die wordt geaudit, conform de beschrijving van de scope van de audit.
- **Auditor:** Uitvoerder van de audit en het bijbehorende gesprek met de audittee op basis van een dienstverleningsovereenkomst en de gewenste insteek. Verantwoordelijk voor de beoordeling op basis van de norm van de audittee. De auditor verkrijgt op basis van een licentieovereenkomst met de Stichting Kwaliteitsinnovatie het recht om audits uit te voeren ten aanzien van deze NIS2 norm.
- **Auditoren:** Individuen of auditorganisaties die voldoen aan de kwalificaties en zijn erkend door de Stichting Kwaliteitsinnovatie.
- **Auditorganisatie:** Ondersteunende organisatie voor de planning en uitvoering van audits.
- **Uitvoeringsorganisatie:** Ondersteunende organisatie voor de activiteiten van de Stichting Kwaliteitsinnovatie, waaronder het inrichten en in stand houden van de registers
- **Register:** Informatie over alle organisaties die hun certificaat hebben behaald of daar de intentie toe hebben via een pre-registratie. Daarnaast het register van gekwalificeerde auditors en hun organisaties.

- **Klachtencommissie:** Een zelfstandig onderdeel van de Stichting Kwaliteitsinnovatie dat een onafhankelijk oordeel geeft over klachten indien verzocht door een auditor of auditee.
- **Steekproeven:** een onaangekondigde toets van gedane audits.

Voor de verschillende termen en activiteiten gelden de volgende **definities**:

- **Informatiebeveiliging:** Het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie waarvoor de auditee (mede) verantwoordelijk is.
- **Cybersecurity:** het deel van de informatiebeveiliging dat zich richt op het beschermen van informatie, systemen, netwerken en applicaties tegen digitale aanvallen.
- **Auditverslag:** het verslag/ rapportage van de auditor, te bewaren voor kwaliteitsdoelen voor 3 jaar en 3 maanden.
- **Beheersmaatregel:** Een beheersmaatregel kan elk proces, beleid, voorziening, werkwijze of andere maatregel zijn waarmee het risico wordt gewijzigd.
- **Bewijsvoering:** alle documenten of systemen die de auditee laat zien of deelt met de auditor.
- **Operational Technology (OT)**: Verzamelnaam voor verschillende systemen die worden gebruikt voor het beheer van operationele processen in de fysieke wereld.
- **Gebruiker:** Belanghebbende met toegang tot één of meer informatiesystemen van de organisatie (bijvoorbeeld: medewerkers, klanten, leveranciers).
- **Dreiging:** potentiële oorzaak van een ongewenst incident dat kan resulteren in schade aan een systeem of een organisatie.
- **Kwetsbaarheid:** Zwak punt van een bedrijfsmiddel of beheersmaatregel waar één of meer dreigingen gebruik van kunnen maken.
- **Incident:** Afzonderlijke of reeks van gebeurtenissen waarvan het zeer waarschijnlijk is dat deze de bedrijfsactiviteiten compromitteren en de informatiebeveiliging in gevaar brengen.
- **Uitbesteden:** Een overeenkomst treffen waarbij een externe partij een deel van een proces van de organisatie uitvoert. De organisatie blijft medeverantwoordelijk voor het uitbestede proces, inclusief de beheersmaatregelen.

6. Reikwijdte

6.1 Doelgroep

Het NIS2 Supply Chain Compliance- en certificeringsschema is een hulpmiddel om aan de NIS2 richtlijn te voldoen.

Alle organisaties die dit hulpmiddel wensen te gebruiken, zijn vrij om dit te doen. Alle organisaties, van groot tot klein, mkb-bedrijven, grote instellingen, zzp'ers, multinationals, stichtingen, verenigingen, coöperaties, federaties en branche-en beroepsorganisaties, etc., ongeacht de sector. In de rapportage wordt de door de auditee opgegeven omschrijving bij preregistratie gevolgd.

De NIS2 richtlijn kent een bredere definitie van veiligheidsrisico's dan bijvoorbeeld de NEN:ISO 27001. Doordat de NIS2 Supply Chain certificering de richtlijn hierin al volgt, werkt deze aanvullend voor organisaties die ook aan dit deel van de richtlijn willen voldoen.

6.2 Passend bij mkb

Dit compliance en certificeringsschema heeft betrekking op alle organisaties die vallen onder de werking van de NIS2 richtlijn en de nationale vertalingen daarvan in wetgeving, in het bijzonder artikel 7 van de Cyberbeveiligingswet en artikel 23 uit de NIS2 Richtlijn. Daarbinnen is er expliciete aandacht voor de doelgroep van mkb-bedrijven en kleinere instellingen.

Naast het beoordelen is ook het activeren van de betrokken (mkb-)bedrijven van wezenlijk belang om deze norm meerwaarde te geven voor alle betrokkenen. Bij de ontwikkeling van Het NIS2 Supply Chain Compliance- en certificeringsschema is nadrukkelijk rekening gehouden met de eis "Zorg ervoor dat mkb-ondernemingen niet worden verplicht kostbare en complexe beproevingsregimes te volgen" (5.4.4) en om "eenvoudige en kosteneffectieve methoden om naleving van de eisen te verifiëren" te eisen. Deze CEN-CENELEC Richtlijn 17 zal onderdeel worden van de test van het schema, met een 0-meting voor de volledige start en een 1-meting.

Er zijn drie niveaus waarop de norm kan worden gehanteerd:

- SC10 op basic niveau
- SC20 op substantial niveau
- SC30 op high niveau

Voor de keuze van de norm is het risiconiveau leidend en de verwachtingen van de ketenpartners. Er is geen dwingende volgorde in het behalen van de normen. Bijvoorbeeld kleinschalige bedrijven en instellingen met een beperkt risico hebben er voldoende aan om de SC10 te doen of daarmee te beginnen. Is er sprake van hogere verwachtingen dan kan ook direct voor de SC20 of SC30 worden gekozen.

De elementen van NIS2 Supply Chain certificering zijn ontleend aan de Europese richtlijn. Dit omvat zowel specifieke beheersmaatregelen als maatregelen die een algemene aanpak voorstaan.

7. Kern van de NIS2: risicoanalyse, risicomanagement, meldplicht, incidentrespons en artikel 21.

Dit NIS2 Supply Chain certificering Compliance en Certificeringsschema is gebaseerd op de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende “maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie.” Deze NIS2 richtlijn treedt op 17 oktober 2024 in Europa in werking.

Het NIS2 Supply Chain Compliance- en certificeringsschema richt zich op de vertrouwelijkheid, integriteit en beschikbaarheid van informatie binnen een organisatie.

Op hoofdlijnen heeft elke organisatie minimaal:

- **Risicoanalyse:** de analyse van risico’s die zich op de korte en langere termijn kunnen voordoen.
- **Risicomanagement:** Inclusief de wijze waarop risico’s worden geadresseerd en de rollen en verantwoordelijkheden die daarbij horen, en de wijze waarop deze verantwoordelijkheden worden gedragen en overgedragen.
- **Meldplicht:** Procedures voor meldplicht aan bevoegde autoriteiten en/of in de toeleveringsketen.
- **Incidentresponsplan:** Elke organisatie dient een incidentresponsplan te hebben, waarin ook de meldplicht staat beschreven.
- In de NIS2 richtlijn staat in artikel 21 een opsomming van maatregelen en aandachtsgebieden:

    a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;

    b) incidentenbehandeling;

    c) bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;

    d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;

    e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;

    f) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico’s te beoordelen;

g) basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;

h) beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;

i) beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;

j) wanneer gepast, het gebruik van multifactor-, authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

De Europese richtlijn bevat hele concrete maatregelen die te mappen zijn op normen. Dat hebben wij ook gedaan - de benadering is ‘rule based’. NIS2 Supply Chain certificering is gemapt op artikel 21 van de NIS2 richtlijn.

Organisaties moeten dus zelf zorgen voor naleving. In de verdere uitwerking daarvan is duidelijk dat het management nauw betrokken moet zijn bij de NIS2.
Van de CEO, het C-level bestuur, wordt leiderschap verwacht. Deze dient goed op de hoogte te zijn van de mogelijke risico’s en daar op actie te nemen.

Dit raakt in ieder geval het betrekken van de IT-, inkoop, juridische en HRM afdelingen. Samen dienen deze afdelingen te zorgen voor afdekking van de drie grote risicogebieden: IT, leveranciers en medewerkers.

Per norm worden de noodzakelijke maatregelen benoemd. Zonder pre-registratie en deelname aan de pre-audit webinar kan er geen audit worden afgenomen.

8. Normen

8.1 Kenmerken

De normen zijn in opdracht van de Stichting Kwaliteitsinnovatie opgesteld door cybersecurityspecialisten, auditoren en andere experts. Daarna is deze vastgesteld door een normcommissie NIS2, bestaande uit vertegenwoordigers van verschillende brancheorganisaties. Bij dit schema hoort ook een vragenlijst voor de beoordeling van het risiconiveau en een dynamische aanpak, zoals beschreven in hoofdstuk 4 over het doel van de norm. De normen hebben elk een eigen kenmerk: SC, wat staat voor ‘Supply Chain certificering’ en een volgnummer: 10, 20 en 30. Per norm is er een normdocument gemaakt.

De nummering is herleidbaar tot de norm, per Supply Chain certificering wordt een deel daaruit geselecteerd. Ook wordt bij elk onderdeel van de norm zichtbaar gemaakt – de ‘mapping’ - hoe de norm zich verhoudt tot andere normen.

Kenmerken en maatregelen van NIS2 SC10 Basic:

Tabel 8.1	Kenmerken NIS2 SC10 Basic	
8.1.1	Uitgangspunten	Minimum drempel, kortdurend, geen specifieke OT- en IT-maatregelen
8.1.2	Maatregelen:	Zie normdocument
8.1.3	Risicobepaling	Vragenlijsten
8.1.4.1	Aantal Auditors	1 per audit
8.1.4.2	Geschatte netto auditduur voor aanvrager/audittee	Zie tabel
8.1.4.3	Geschatte auditduur voor auditor (bij voldoende)	Zie tabel 8.5

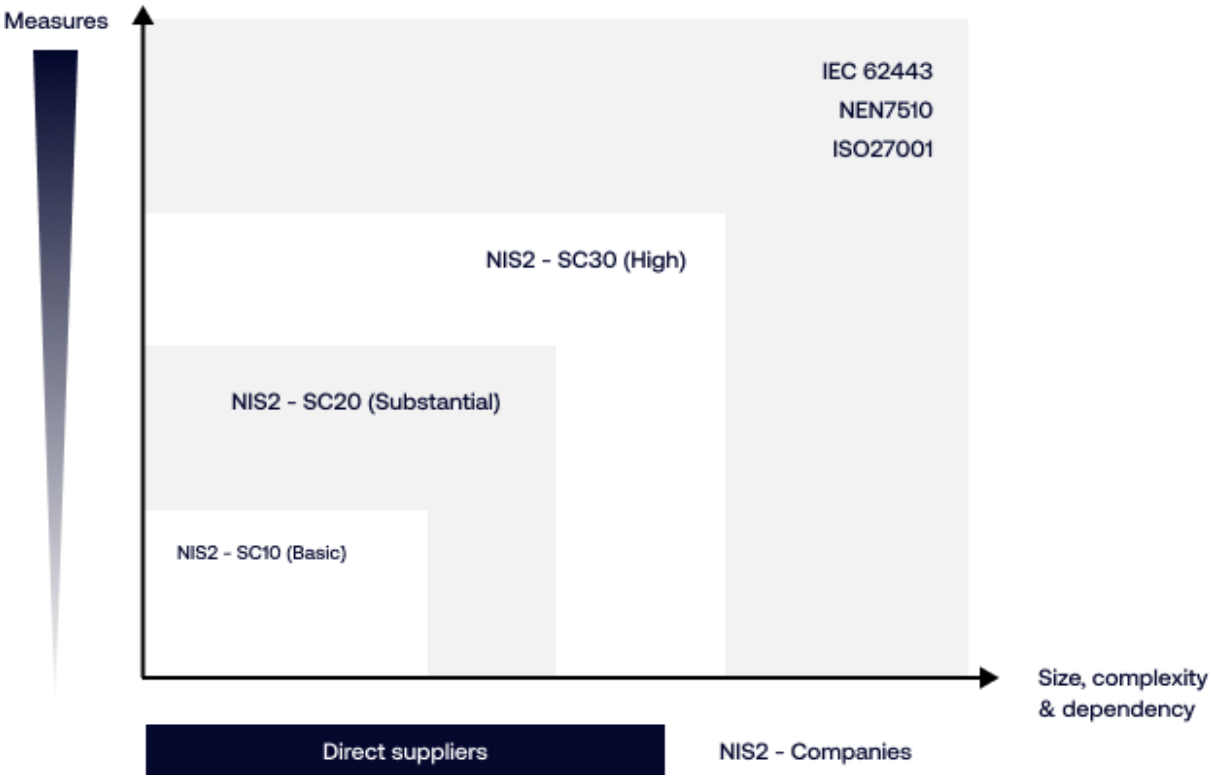
Kenmerken en maatregelen van NIS2 SC20 Substantial:

Tabel 8.2	Kenmerken NIS2 SC20 Substantial	
8.2.1	Uitgangspunten	Logische doorloop op Basic, versterken P-D-C-A, technologische OT en IT-maatregelen
8.2.2	Maatregelen	Zie normdocument
8.2.3	Risicobepaling	Vragenlijsten + verslag mogelijke verbeteringen
8.2.4.1	Aantal Auditors	1-2
8.2.4.2	Geschatte auditduur voor aanvrager/audittee	Zie tabel
8.2.4.3	Geschatte auditduur voor auditor (bij voldoende)	Zie tabel 8.5

Kenmerken en maatregelen van NIS2 SC30 High:

Tabel 8.3	Kenmerken NIS2 SC30 High	
8.3.1	Uitgangspunten	Logische doorloop op Substantial, versterken P-D-C-A, uitgebreide aandacht voor OT- en IT-maatregelen
8.3.2	Maatregelen	Zie hoofdstuk 22
8.3.3	Risicobepaling	Vragenlijsten + verslag van mogelijke verbeteringen
8.3.4.1	Aantal Auditors	1-2
8.3.4.2	Geschatte auditduur voor aanvrager/ audittee	Zie tabel 8.3.2 of Werkwijzer voor de audit
8.3.4.3	Geschatte auditduur voor auditor	Zie tabel 8.5

8.2 Groeiladder



De Europese Commissie heeft in haar Europese NIS2 richtlijn de toeleveringsketen (‘supply chain’) benoemd. Dit impliceert uitdagingen op vele niveaus in het bedrijfsleven en de samenleving als geheel. Een veel groter aantal bedrijven en organisaties worden daardoor geraakt. Niet alleen de vaak wat grotere NIS2 organisaties en bedrijven, maar ook de minder grote bedrijven en mkb-bedrijven (toeleveranciers). ENISA werkt in het kader van andere cybersecurityrichtlijnen met een geadapteerde verwerking op meerdere niveaus. De basisveronderstelling is dat mkb-bedrijven niet direct aan dezelfde conformiteit standaarden kunnen voldoen als grote multinationals.

Er zijn normen op drie niveaus geformuleerd. Deze niveaus vormen een ladder voor bedrijven die onder de scope vallen. Zo kunnen ze zich op dynamische wijze ontwikkelen naar het hogere veiligheidsniveaus: van Basic via Substantial naar High. Vervolgens kunnen organisaties desgewenst aansluiten op o.a. ISO27001/NEN7510 en andere vergelijkbare normen.

8.3 Looptijd en tijdsduur beoordeling

8.3.1 Looptijd

De audit kent een 3-jaarlijkse herhaalcyclus. Bij de 3 niveaus horen ook verschillende beoordelingsniveaus.

Beoordeling	Basis	Substantial	High
Norm	NIS2 SC10	NIS2 SC20	NIS2 SC30
Type beoordeling	Certificering	Certificering	Certificering
Beoordelingsmethode	Certificering van zelfevaluatie en/of maatregelen op afstand	Certificering van zelfevaluatie met beoordeling ter plaatse	Certificatie audit
Beoordeling door	1 auditor met omschreven kwalificaties*	1-2 auditoren met omschreven kwalificaties*	1-2 auditoren geaccrediteerd auditbureau
Accreditatie standaard	ISO/TEC 17029 en/of toestemming van de Stichting Kwaliteitsinnovatie	ISO/TEC 17029 en/of ISO/TEC 17021 en/of toestemming van de Stichting Kwaliteitsinnovatie	ISO/TEC 17021-1 en/of toestemming van de Stichting Kwaliteitsinnovatie.
Bewijs van voldoen	Afgeronde audit of diagnose met positief resultaat	Afgeronde audit met positief resultaat	Afgeronde audit met positief resultaat

- Aan onvolkomenheden, ‘minors’, worden geen consequenties verbonden. Herstel in 3 maanden moet worden aangetoond aan auditor.
- Aan elke auditor wordt een reviewauditor gekoppeld. Bij meer omvangrijke bedrijven kunnen ook meer auditoren worden ingezet (zie hoofdstuk 10).

8.3.2 Indicatietabel tijdsduur per audit

Tabel A: Basis aantal audituren			
FTE	**SC10**	**SC20**	**SC30**
mkb ≤ 10	4	8	20
mkb 11 - 25	8	12	24
mkb 26 - 100	16	20	36
mkb 100 - 250	24	32	40
mkb > 250	*op aanvraag*	*op aanvraag*	*op aanvraag*
NIS2 org <25	12	16	28
NIS2 org <=100	20	24	40
NIS2 org ≤ 500	32	40	48
NIS2 org > 500	*op aanvraag*	*op aanvraag*	*op aanvraag*

Tabel B: extra audituren locaties / rechtspersonen			
B.1 IT NIET centraal geregeld			
Locaties / rechtspersonen 2 < 5	4	8	12
Locaties / rechtspersonen 6 - 10	8	16	24
Locaties / rechtspersonen 11 - 25	16	32	48
Locaties / rechtspersonen 26 - 100	*op aanvraag*	*op aanvraag*	*op aanvraag*
Locaties / rechtspersonen > 100	*op aanvraag*	*op aanvraag*	*op aanvraag*
B.2 IT WEL centraal geregeld			
Locaties / rechtspersonen 2 < 5	2	4	6
Locaties / rechtspersonen 6 - 10	4	8	12
Locaties / rechtspersonen 11 - 25	8	16	24
Locaties / rechtspersonen 26 - 100	*op aanvraag*	*op aanvraag*	*op aanvraag*
Locaties / rechtspersonen > 100	*op aanvraag*	*op aanvraag*	*op aanvraag*

Tabel C: korting ter voorkoming van dubbele toetsing			
Is de audittee in bezit van een ISO27001 of NEN7510 certificering?	-60%	-60%	-60%

Hoe werkt bovenstaande?
Neem de waarde uit Tabel A.
Tel daar de waarde van Tabel B1 óf B2 bij op.
Het eindresultaat is het totaal aantal audituren.

Online en of op locatie?
Audits zijn volledig online bij SC10.

Bij SC20 zijn audits online. Bij meer dan 24 uur audittijd geldt minimaal één dagdeel op locatie.
Bij SC30 zijn audits online én op locatie. Bij meer dan 24 uur audittijd geldt minimaal één volledige dag op locatie.

Locaties / rechtspersonen:
Neem de hoogste van de 2. Tel alleen de rechtspersonen die men wil laten certificeren.

Audittijd:
Audittijd is altijd minimaal 4 uur
Audittijd is een optelsom van bovenstaande tabellen. De audittijd is inclusief voorbereiding en verslaglegging.

Op basis van het bovenstaande kunnen inschattingen worden gemaakt van de benodigde audittijd. Daarbij wordt een onderscheid gemaakt tussen de omvang van de deelnemende bedrijven en instellingen, om de vraag of het om een bedrijf en instelling gaat die verplicht deelneemt aan de NIS2 richtlijn en om het aantal vestigingen.

Indien een bedrijf of instelling al een andere cybersecuritynorm heeft, kan dit van invloed zijn op de te besteden tijd. Zie Mapping 9.3.

Voor een toelichting over de exacte tijden en inhoud van de audits, inclusief het certificaat uitreikingsproces, zie Werkwijzer voor de audit. Dit document wordt, samen met een digitale audittool, ter beschikking gesteld aan auditorganisaties die namens de Stichting Kwaliteitsinnovatie zijn aangeduid als auditors.

Indien tijdens de audit op maximaal twee onderdelen een onvoldoende wordt gescoord, krijgt de auditee de mogelijkheid om deze specifieke punten binnen een periode van maximaal drie maanden te herstellen.

Voor elk onvoldoende onderdeel worden voor de extra beoordeling twee extra uren in rekening gebracht. Het certificaat wordt wel direct verstrekt zodra de Stichting het positieve advies van de auditor overneemt, op voorwaarde dat de betreffende maatregelen binnen de gestelde termijn aantoonbaar zijn geïmplementeerd. Indien geen bewijs van herstel wordt aangeleverd binnen deze termijn, wordt de certificering ingetrokken.

9. Relatie met andere normen en mapping

9.1 Relatie met andere normen

Het NIS2 Supply Chain certificaat Compliance en Certificatieschema is gebaseerd op de Network and Information Security Directive 2 (NIS2) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022L2555).

Bij de invulling is gekeken naar gangbare beveiligingskeuzes en aanbevelingen door cybersecurityspecialisten. Deze maatregelen zijn wijdverspreid in de huidige cybersecuritywereld en komen terug in de meeste gangbare stelsels, normen, schema's en standaarden.

Binnen dit schema zijn eigen maatregelen gemaakt op basis van input van vele experts en vertegenwoordigers van branches, rekening houdend met maatregelen die de meeste veiligheid en de minste lasten toevoegen in combinatie met de verplichtingen zoals beschreven in de NIS2.

9.2 Mapping met andere normen, standaarden en frameworks

Niemand werkt in een vacuüm. Alle bedrijven hebben al maatregelen getroffen voor hun cybersecurity, bewust of onbewust, via normen of samen met hun IT-bedrijf. Dus niemand start vanaf nul. Er is een mapping gemaakt op de meest gangbare normen. Deze mapping is verwerkt in elk van de NIS2 SC normen.

Tabel 9.2	Mapping	Versiedatum:
Tabel 9.2.1	Mapping SC - NEN-ISO 27001	
Tabel 9.2.2	NIS2 SC10 Basic	18-04-2025
Tabel 9.2.2	NIS2 SC 20 Substantial	18-04-2025
Tabel 9.2.3	NIS2 SC30 High	18-04-2025

9.3 Vrijstelling en dubbel werk voorkomen door Mapping

Als een bedrijf of instelling in aanmerking wil komen voor Het NIS2 Supply Chain certificaat en er is al een andere norm behaald, dan hoeven ze de onderdelen die al aantoonbaar zijn behaald in de andere norm, niet opnieuw te doen. Via Mapping kan men vaststellen welke onderdelen met elkaar vergelijkbaar zijn. Reeds genomen maatregelen hoeven niet opnieuw gedaan te worden en zijn vrijgesteld van auditplicht, mits de norm binnen 2 jaar voor datum is beoordeeld. Voor nadere details zie de Werkwijzer voor de audit.

10. Kwalificaties voor beoordeling

10.1 Kwalificaties

Er wordt een onderscheid gemaakt in de deskundigheidseisen voor auditors voor het auditen van de Basic, Substantial en High kwalificatie. De uitvoering van audits wordt in handen gegeven van door de Stichting Kwaliteitsinnovatie erkende auditorganisaties die tot taak hebben auditoren in te zetten en de kwalificaties van de in te zetten auditoren te bewaken. Er wordt een onderscheid gemaakt tussen:

- Auditorganisaties die op individuele basis gekwalificeerd zijn om als auditor op te treden en aantoonbaar over de benodigde normkennis en audittechnieken beschikken. Deze worden na een opleiding door de Stichting Kwaliteitsinnovatie erkend als auditor en zijn gerechtigd om de SC10 en deels de SC20 (de bedrijven en organisaties die niet direct onder de NIS2 vallen) te auditeren en/of te diagnosticeren.
- Auditorganisaties die geaccrediteerde certificerende instellingen (CI's) zijn en als zodanig voor audits gekwalificeerde medewerkers inzetten, inclusief voldoende ondersteuning. De kwalificaties blijken op basis van de (zie tabel met normen). Deze licentiehouders zijn gerechtigd om alle NIS2 SC normen te auditeren.

Alleen auditoren, auditorganisaties en CI's die zijn erkend door de stichting Kwaliteitsinnovatie kunnen NIS2 SC zelfstandig audits doen en voor hun audittee een NIS2 Certificaat aanvragen en uitreiken. Erkenning kan aangevraagd worden via de Stichting Kwaliteitsinnovatie.

In het document 'Werkwijze van de audit' en de daarbij behorende digitale audittool is de wijze waarop de audit dient te worden uitgevoerd nader uitgewerkt.

11. Opleiding auditoren

De NIS2 SC normen hechten veel waarde aan goed opgeleide medewerkers. Bij de bedrijven zelf is opleiding in cyberrisico's een vast onderdeel, ook voor de directieleden. Voor de auditoren geldt datzelfde.

De opleiding is een dagdeel en richt zich vooral op het auditgesprek. Kennis over de NIS2 normen en wijze van beoordelen en technische kennis over cybersecurity dient al aanwezig te zijn.

Onderwerpen die sterk de competentie van de auditor bepalen en in de opleiding aan de orde komen zijn:

- Normkennis, toepassing technische kennis en beoordeling risico's
- Audittool en proces van de audit
- Gespreksvoering
- Stimulering
- Rapportage

Voor de licentiehouders (certificerende instellingen/schemabeheerders) worden de eisen vastgelegd in een overeenkomst. Deze omvatten ook de kwalificaties.

In het document 'Werkwijze van de audit' wordt dit nader uitgewerkt.

12. Aanmelden en aanvragen certificering

Bedrijven en organisaties die Het NIS2 Supply Chain Compliance- en certificeringsschema willen halen, dienen de volgende stappen te doorlopen:

- Doe de verplichte pre-registratie via de NIS2 SC website.
- Doorloop stappen en maatregelen zoals beschreven in de norm.
- Indien nodig, schakel externe ondersteuning in. Er zijn vele partijen die kennis hebben van de materie en kunnen ondersteunen.
- Neem deel aan de verplichte pre-auditwebinar en oer waar nodig aanvullingen en/of correcties uit.
- Selecteer een audit organisatie.
- Sluit een overeenkomst af met de audit-instelling van uw keuze.
- De audit instelling doet de toetsing of diagnose en beoordeelt of uw organisatie voldoet aan de eisen op basis van gedocumenteerde informatie, interviews en waarnemingen.
- Voer binnen 3 maanden herstel uit als daar aanleiding toe is.
- Het certificaat wordt verstrekt als de certificerende instelling oordeelt dat uw organisatie voldoet aan de eisen van de NIS2 SC.
- Het certificaat heeft een geldigheidsduur van drie jaar.

12.1 Aanmelden voor certificering via pre-registratie

Bij aanmelding wordt het bedrijf of de instelling door de Stichting Kwaliteitsinnovatie geregistreerd. Dit kan al direct via een zogenaamde ‘pre-registratie’. In de bevestiging wordt nadere informatie gegeven over het proces. De aanmelding wordt definitief in behandeling genomen als de aanvraag alle benodigde elementen omvat.

12.2 Aanvraag voor certificering

De aanvraag voor certificering bij de Stichting Kwaliteitsinnovatie bevat de volgende gegevens:

- Organisatienaam, volledig adres, naam van de contactpersoon, contactgegevens en het ondernemingsnummer van de organisatie.
- Het registratienummer (verkregen bij de pre-registratie)
- Het aantal medewerkers van de organisatie.
- De wijze waarop de informatietechnologie is georganiseerd in de organisatie: centraal of decentraal
- Datum van de beoordeling.
- De versie van Het NIS2 Supply Chain Compliance- en certificeringsschema waarvoor men gecertificeerd wenst te worden.
- Een advies of diagnose van de auditor/audit organisatie aan de Stichting Kwaliteitsinnovatie dat auditee voldoet aan de vereisten van Het NIS2 Supply Chain certificaat zoals vastgelegd in Het NIS2 Supply Chain certificaat Compliance en Certificeringsschema.

12.3 Elementen van de audit

In elke audit zijn de volgende elementen in het proces herkenbaar:

Tabel 12.2.1	Proces: uitvoering audit	Vanuit perspectief auditor:
1	Onderzoeksfase: evaluatie van aangeleverde bewijsstukken	Beoordelen van bewijsstukken.
2	Voeren auditgesprek	Risk-based bespreken van mogelijke tekortkomingen en risico's. Toetsen per normelement op basis van het gekozen Supply Chain certificering.
3	Afronden, terugkoppeling en stimuleren	Afronden gesprek, terugkoppeling, stimuleren waar nodig.
4	Rapportage	Indienen advies of diagnose bij de Stichting Kwaliteitsinnovatie voor aanvraag en beoordeling certificering
5.	Uitreiken certificering of herbeoordeling (review)	Evalueren

12.4 Beoordeling van de audit

De initiële beoordeling wordt gedaan aan de hand van alle aangeleverde bewijsstukken. Daarna zal er een beoordeling ter plaatse of op afstand plaatsvinden waarbij via vragen en een gesprek een volledig beeld kan worden gevormd van de mate waarin een organisatie voldoet aan de minimale eisen om certificering te verkrijgen.

Om de drie jaar wordt een volledige beoordeling uitgevoerd. Elke beoordeling heeft een score.

Elke norm kent verplichte maatregelen die in de audit zeker op orde moeten zijn en overige maatregelen. Een optimale audit kent een evenwicht tussen het beoordelen van maatregelen en het op stimulerende wijze bespreken van bevindingen en daarin kan het geven van een dergelijke ondergrens auditoren helpen in het maken van hun keuze. De verplichte maatregelen worden gepubliceerd in de Werkwijzer voor de audi.

De score voor de verplichte onderdelen dient minimaal een voldoende te zijn (6 of hoger op 10) om een certificering te kunnen ontvangen. Van alle overige onderdelen mogen individuele onderdelen een onvoldoende scoren maar het totaal van alle maatregelen moet een gemiddelde hebben van 6,0 op 10 of hoger. Details staan in de Werkwijzer voor de audit.

12.5 Rapportage van de audit

De rapportage van een audit omvat:

- Vaststelling identiteit aanvrager/auditee en datum(s) toetsing in combinatie met het verkregen registratienummer.
- Omschrijving beoordeelde maatregelen en het oordeel hierover in de vorm van een certificatieadvies.
- Betrokken documenten en personen/functies.
- Uitkomsten risicoanalyse en verwachting over aanpak uitkomsten door auditee.
- De uitkomsten en bewijsmiddelen van de geauditeerde of gediagnostiseerde onderdelen van de norm die van toepassing zijn en in het gesprek aan de orde komen en leiden tot een uitspraak over voldoen of niet voldoen. Deze dienen ten minste drie jaar en drie maanden bewaard worden ten behoeve van kwaliteitsdoeleinden.
- Uitspraken over voldoen of niet voldoen en de daaraan verbonden termijn om verbeteringen aan te brengen, met in achtneming van de daarbij horende termijn van uiterlijk 3 maanden.
- Eventuele aanwijzingen ter stimulering in de rapportage in relatie tot het auditresultaat.
- Overige zaken en/of opmerkingen die voor een evaluatie relevant zijn.
- De rapportage is uitsluitend bedoeld voor de auditor en de auditee en enkel inzichtelijk voor personen verantwoordelijk voor de kwaliteitsbeoordeling op de wijze zoals in hoofdstuk 17 over kwaliteitsborging beschreven.

13. Dynamisch karakter van de norm

13.1 Stimuleren voor verdere groei

In het verlengde van de audit kunnen stimulerende maatregelen worden voorgesteld op alle essentiële aspecten van de audit: risicoanalyse, norm en in het kader van het oordeel. Dit in lijn met de stimulerende doelstelling van de aanpak: na het niveau Basic is er nog een weg op de ladder te gaan en daar willen we bedrijven en organisaties bij ondersteunen. De Stichting Kwaliteitsinnovatie legt een lijst aan met deze maatregelen, inclusief een korte beschrijving van mogelijke relevantie. In het auditrapport kan hiernaar worden verwezen.

Deze stimulerende maatregelen uit de lijst liggen in het verlengde van de uitkomsten van de audit, wijzen in de richting van maatregelen die geschikt zijn voor opvolgende normen als de SC20 en SC30 en omvatten geen advies of verplichting.

Daarnaast ontvangt elk gecertificeerde bedrijf of instelling elk jaar activiteiten aangereikt die ondersteunen om naar een volgende stap op de auditladder te komen in termen van cybersecurity.

Tabel 13.1	Proces: stimulerende maatregelen
13.1.1	Lijst stimulerende maatregelen
13.1.2	Tijdens audit: selectie stimulerende maatregelen
13.1.3	Verwijzen naar ondersteuning en opleiding
13.1.4	Resultaten volgen
13.1.5	Delen met een digitaal platform

13.2 Werkingstermijn van de norm

Een certificaat voor het voldoen aan de normen van Q10, SC20 en SC30 wordt verstrekt voor de duur van 3 jaar. In die tijd moet de norm wel worden onderhouden. Dit geldt temeer daar de ontwikkelingen in het veld van cyberweerbaarheid bijzonder snel gaan en daar ontwikkelingen als AI (Artificial Intelligence) bijkomen en hun doorwerking hebben. Om die reden is een geldigheidstermijn van langer dan 3 jaar niet passend. Daarnaast verwachten wij dat deze dynamiek vraagt om het geregeld onderhouden van de norm en haar toepassing. Bedrijven dienen er dus rekening mee te houden dat er voor elke norm tussentijds elementen bij kunnen komen en zeker voor de SC30 kunnen dat er meerdere zijn.

Bedrijven worden gevraagd om rekening met deze aanpassingen te houden, ook met het oog op eventuele hercertificering. Voor de SC30 kan vanaf 2026 sprake zijn van een jaarlijkse toetsing als de ontwikkelingen daar aanleiding toe geven.

14. Eisen aan digitale beveiliging

ICT-platformen en programma's die Het NIS2 Supply Chain certificaat commercieel exploiteren, dienen zeer goed beveiligd te zijn. Ze dienen te worden gecontroleerd op veiligheid via pentests en dienen het bewijs hiervan te overleggen. Specifieke beveiligingsafspraken zullen worden gemaakt met elke partij die Het NIS2 Supply Chain certificaat gaat voeren en/of auditeren. Daarnaast worden afspraken vastgelegd in de 'Werkwijzer voor de audit'.

Wij zullen vooral kijken naar en aandacht hebben voor de volgende technische en organisatorische zaken als wij met een GRC en/of audit partij een samenwerking afspreken. In die gevallen is er sprake van en/of rekening gehouden met:

- Beveiligde gegevensuitwisseling met audittee.
- Veilige inlog (MFA of vergelijkbaar).
- Toegang tot audittee gegevens uitsluitend voorbehouden aan de auditor.
- Aantonen dat de applicatie aantoonbaar is beschermd, bijvoorbeeld door het voorleggen van een PEN-test resultaat.
- Het aantoonbaar beschikken over passende cybersecurity certificering of daarvan zijn vrijgesteld op basis van aantoonbare ervaring.

15. Juridische kaders

Bij de toepassing en toetsing van het schema moet rekening worden gehouden met gebruik in verschillende domeinen en de daarbij horende juridische kaders:

- Toetsing op de governance van de (oordeelsvorming) ten aanzien van de audits voor de Stichting Kwaliteitsinnovatie.
- De laatste versie van de NIS2 richtlijn in de Engelse taal is de geldende versie voor de lidstaten van de Europese Unie.
  In de lidstaten van de Europese Unie kan de NIS2 richtlijn vertaald worden naar eigen wet- en regelgeving. Het is aan de betrokken bedrijven en instellingen om deze nationale toespitsingen te volgen en aan de licentiehouder(s) om deze bij de audit aanvullend te hanteren. Het NIS2 Supply Chain Compliance- en certificeringsschema moet dus uitsluitend gezien worden als een generiek hulpmiddel en niet als “de vertaling van de NIS2 wetgeving” in een lidstaat.
- Relevante Europese regelgeving, in het bijzonder NIS2 en aanpalende regelgeving in ontwikkeling op het terrein van privacy en artificiële intelligentie, hoort daar nadrukkelijk ook bij.
- Branche-specifieke regelgeving van de deelnemende bedrijven, voor zover deze dwingen tot afwijkende hantering van de binnen dit schema gehanteerde normen, horen hier ook bij.

16. Gebruik van de norm en logo door certificaathouders

	Gebruik keurmerk		
16.1	Omschrijving keurmerk en logo		Donkerblauw schild op witte ondergrond, met vierkant met daarin vink-teken. Daarnaast naam 'NIS2' en daaronder 'Supply Chain certificering'.
16.2	Gebruiksvoorwaarden keurmerk derden		Gebruik van het keurmerk en de daar aan verbonden uitingen uitsluitend na voorafgaande toestemming door de Stichting Kwaliteitsinnovatie, Noordwijk, Nederland. Verzoeken richten tot de Stichting Kwaliteitsinnovatie per mail: info@nis2supplychain.eu.
16.3	Copyrights en licenties		© Alle intellectuele eigendomsrechten, waaronder auteursrechten, handelsmerken en ontwerprechten in en op deze cybersecurity norm zijn voorbehouden. Zonder voorafgaande toestemming is het niet toegestaan om enig deel van dit document te kopiëren, wijzigen of anderszins te gebruiken. Dit document is dynamisch van aard. Dit is versie 3.1 van 8 april 2025. Raadpleeg de meest recente versie op www.nis2supplychain.eu.

17. Oordelen over de werking van het stelsel

Oordelen over de werking van het op basis van dit schema ingerichte stelsel vinden plaats op het niveau van:

- Evaluaties per audit
- Klachten en bezwaar
- Steekproefsgewijze evaluatie

17.1 Evaluaties per audit

Digitale evaluaties worden aan de hand van de ‘evaluatiecriteria NIS2 SC audit’ en ‘evaluatiecriteria NIS2 SC auditor’ uitgevoerd bij deelnemers en auditoren, met mogelijkheden voor directe feedback en suggesties. Rapportage, analyse, aanbevelingen en uitvoering van de verbeteracties worden door de Stichting Kwaliteitsinnovatie uitgevoerd.

17.2 Klachten en bezwaar

Aan de norm is een klachten- en geschillencommissie verbonden. Leden daarvan komen onder andere uit deelnemende brancheverenigingen. Deze commissie is nog in oprichting en is onafhankelijk van elk oordeel door de Stichting Kwaliteitsinnovatie.

Klachten kunnen op een toegankelijke manier worden gericht aan en verzameld door de Stichting Kwaliteitsinnovatie. De Stichting Kwaliteitsinnovatie streeft naar een reactietermijn van een week en zal bij een gegronde klacht spoedig maatregelen treffen.

De Stichting Kwaliteitsinnovatie analyseert jaarlijks in een kwaliteitsrapportage eventuele klachten en maakt deze onderdeel van de evaluatie van het stelsel en brengt deze, voorzien van aanbevelingen, ter kennis van de stichting.

17.3 Steekproefsgewijze evaluatie

Steekproefsgewijze evaluatie is gericht op een bredere inschatting van de meerwaarde van de aanpak. Het omvat ten minste:

- Evaluatie op niveau deelnemers.
- Evaluatie op niveau auditors.
- Evaluatie op niveau licentiehouders (naar aard activiteiten en aanpassing op NIS2 aanpak).
- Evaluatie op contextniveau (wijziging normen, bepaling balans tussen stimuleren en controleren en aanpalende ontwikkelingen zoals op het gebied van privacy, inzet AI en dergelijke).

18. Uitzonderingen, aandachtspunten, volume, toekomstige ontwikkelingen en groei.

Omschreven kwalificaties

In hoofdstuk 8.3 staat dat audits gedaan kunnen worden door partijen met omschreven kwalificaties. Wij hanteren de aanname dat het nodig zal zijn om een onderscheid te maken tussen geaccrediteerde cybersecurity auditors, ICT-auditors, seniors, mediors en juniors in elke mogelijke combinatie. Het beschikbare aantal auditoren mag geen bottleneck worden voor de implementatie van NIS2 in Europa. Uitsluitend auditoren en auditpartijen die erkend zijn door de Stichting Kwaliteitsinnovatie kunnen NIS2 SC audit doen.

Uitzonderingen

De Stichting Kwaliteitsinnovatie behoudt zich nadrukkelijk het recht voor om afwijkingen toe te staan als situaties daartoe aanleiding geven.

Self-assessments

De mogelijkheid bestaat voor bedrijven en organisaties om een zelfevaluatie te doen. Daaruit zou de behoefte kunnen ontstaan om daar een tijdelijke status aan te ontlenen. Bijvoorbeeld in geval van wachtlijsten voor audits. Alleen in dat geval kunnen bedrijven en organisaties een tijdelijke status aanvragen via een pre-registratie. De Stichting Kwaliteitsinnovatie behoudt zich nadrukkelijk het recht voor om afwijkingen toe te staan als situaties daartoe aanleiding geven.

Europees karakter

Certificering op basis van de NIS2 Supply Chain certificering is ook geldig voor de supply chain in andere landen binnen de Europese Unie. Met het oog hierop zijn alle teksten vertaald in de talen van de verschillende landen van de Europese Unie. Wel kan het zijn dat lokale en nationale kaders voor cybersecurity van toepassing zijn. Het is verstandig zich daarop te oriënteren.

Aandachtpunten

Snelle ontwikkelingen in het veld van cybersecurity, zoals de inzet van AI door criminelen, de ontwikkelingen van Quantum computing en de opkomst van nieuwe snellere manieren waarop cyberincidenten zich ontwikkelen, eisen continue aandacht van de Stichting Kwaliteitsinnovatie. Daarom krijgt elke norm een dynamisch karakter, zoals omschreven in hoofdstuk 13. Samenwerking is essentieel en wij doen een beroep op alle markt- en kennispartijen om relevante informatie met ons te delen.

19. Geheimhouding en gegevensbescherming

Alle partijen benoemd in het schema zijn gehouden aan geheimhouding over klanten en werkzaamheden en ondertekenen daartoe een verklaring bij het aangaan van een overeenkomst voor korte of lange duur of indiensttreding.

De Stichting Kwaliteitsinnovatie valt onder de wettelijke regels die door de Algemene Verordening Gegevensbescherming (AVG/GDPR) worden gesteld aan de verwerking van persoonsgegevens. De organisatie voldoet aan de eisen die door de AVG worden gesteld.

Alle normteksten zijn te vinden op https://nis2supplychain.eu/nis2-supply-chain/

20. Copyright en disclaimer

Hoewel de maatregelen, opgenomen in Het NIS2 Supply Chain certificaat en gerelateerde overzicht van maatregelen, zijn ontwikkeld door experts en met de grootst mogelijke zorg zijn samengesteld, worden geen garanties gegeven met betrekking tot de correctheid, volledigheid, betrouwbaarheid, geschiktheid, of beschikbaarheid van Het NIS2 Supply Chain certificaat en de daarin opgenomen informatie, producten, diensten, of gerelateerde grafieken. Het gebruik van Het NIS2 Supply Chain certificaat en gerelateerde overzicht van maatregelen zijn volledig voor het risico van de gebruiker. Elke aansprakelijkheid voor schade, direct of indirect, voortvloeiend uit of in enig opzicht verband houdend met het gebruik van Het NIS2 Supply Chain certificaat en gerelateerde overzicht van maatregelen wordt uitgesloten.

In Het NIS2 Supply Chain certificaat mapping overzicht kunnen verwijzingen zijn opgenomen naar andere standaarden, waaronder ISO 27001:2022 en NEN 7510, uitsluitend voor informatieve doeleinden en om mogelijke samenhang of raakvlakken te identificeren. Deze verwijzingen impliceren geen associatie of goedkeuring van de inhoud van de andere standaarden. Het NIS2 Supply Chain certificaat en gerelateerde overzicht van maatregelen en de genoemde andere standaarden zijn afzonderlijke en unieke documenten. Alle rechten met betrekking tot andere standaarden die in het document worden genoemd, behoren toe aan de respectieve rechtmatige eigenaren van die standaarden.

21. Nationale implementatie van NIS2

Binnen de Europese Unie is de NIS2-richtlijn opgesteld om de digitale weerbaarheid te versterken. Het is echter belangrijk om te begrijpen dat een richtlijn geen verordening is. Waar een verordening direct van toepassing is in alle lidstaten, stelt een richtlijn doelstellingen vast die door elk land afzonderlijk moeten worden omgezet in nationale wetgeving. Dit geeft lidstaten de enige ruimte om zelf te bepalen hoe zij de richtlijn implementeren.

Die vrijheid leidt ertoe dat er verschillen kunnen ontstaan tussen landen. Zo kiezen lidstaten zelf welke instantie het toezicht op naleving op zich neemt. Ook de invulling van sancties is nationaal bepaald: de richtlijn stelt weliswaar een bovengrens aan boetes vast, maar landen kunnen daarbinnen zelf bepalen hoe streng of soepel ze handhaven, zolang de sancties maar doeltreffend, afschrikkend en evenredig zijn. Daarnaast mogen landen aanvullende eisen stellen aan bedrijven, boven op de minimumeisen van de richtlijn.

Een ander belangrijk punt is dat lidstaten ruimte hebben om eigen keuzes te maken in de sectorindeling. De richtlijn bevat een Europese lijst van essentiële en belangrijke entiteiten, maar landen mogen daar sectoren of bedrijfstypen aan toevoegen. Tot slot is de manier waarop bedrijven hun naleving aantonen — bijvoorbeeld via audits of certificaten — niet door de EU vastgelegd, waardoor dit per land kan verschillen.

Voor bedrijven die grensoverschrijdend opereren, betekent deze nationale vrijheid een toename in complexiteit.

Wij streven ernaar om de NIS2SC in alle landen zoveel mogelijk gelijk te houden. Tegelijkertijd is dat soms niet mogelijk of wenselijk.

Nadat de NIS2 in alle landen is geïmplementeerd zullen wij starten met het in kaart brengen van de afwijkingen per land. Tot dan zullen wij uitsluitend indicaties opnemen zover die bij os bekend zijn.

Wij nodigen iedereen uit om ons afwijkingen die al gelden in de diverse landen bij ons te melden via de website supplychain.eu

Indicaties van afwijkingen in Europa:

Nederland:

Het nu voorliggende concept van de Cyberbeveiligingswet (Cbw)[1], in het bijzonder artikel 7, het Cyberbeveiligingsbesluit (Cbb)[2] en het Besluit Weerbaarheid kritieke entiteiten (Bwke)[3]. Het genoemde artikel 7 legt de ‘kritieke entiteit’ de plicht op haar rechtstreekse leveranciers en dienstverleners te identificeren en daar beleid op te maken zodat risico’s beperkt kunnen worden. Omdat voorzienbaar is dat het hier vooral om het mkb gaat en hier een reeks van verplichtingen en verantwoordelijkheden voor hen uit voort vloeien (en hun leveranciers) is dit certificeringsschema

[1] Cyberveiligheidswet, consultatieversie 2025
[2] Cyberbeveiligingsbesluit, consultatieversie 2025
[3] Besluit Weerbaarheid kritieke entiteiten, consultatieversie 2025

ontwikkeling om de verkleining van de risico's ook voor het mkb te realiseren en dat zo te doen dat de regeldruk zo gering mogelijk blijft.

Training van bestuurders onder de Cyberbeveiligingswet: stand van zaken

In de conceptteksten van de Nederlandse Cyberbeveiligingswet (Cbw) en de bijbehorende Algemene Maatregel van Bestuur (AMvB) is opgenomen dat bestuurders van essentiële en belangrijke entiteiten over voldoende kennis en vaardigheden moeten beschikken om cyberrisico's te herkennen, te begrijpen en hierop te kunnen sturen. Daarmee sluit Nederland aan bij de NIS2-richtlijn, die stelt dat de verantwoordelijkheid voor cyberweerbaarheid bij de hoogste managementlaag ligt.

De concept-AMvB suggereert dat er mogelijk nadere eisen worden gesteld aan de inhoud en vorm van deze trainingen. Denk hierbij aan de inzet van een bevoegde trainer, aantoonbare aanwezigheid tijdens de training, en het verkrijgen van een certificaat als bewijs. Op dit moment is er echter nog geen definitieve duidelijkheid over de exacte invulling van deze verplichting.

De internetconsultatie over de AMvB is inmiddels afgerond en er zijn veel reacties binnengekomen, met name op dit onderdeel. Het ministerie van Justitie en Veiligheid werkt momenteel aan de beoordeling van deze reacties. Op basis daarvan wordt besloten of en in hoeverre de regels rondom de trainingseisen voor bestuurders worden aangepast.

Het is belangrijk voor organisaties om zich bewust te zijn van deze aankomende verplichting en alvast na te denken over passende maatregelen, ook al is de definitieve wet- en regelgeving nog in ontwikkeling.