



- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11

Blijf in business met het NIS2 Quality Mark

Aantoonbaar je cybersecurity op orde

Veilig samenwerken in de keten is essentieel voor alle bedrijven

De NIS2 richtlijn is bedoeld om Europa beter te beschermen tegen cyberaanvallen. Het doel? De veiligheid van essentiële organisaties zoals ziekenhuizen, drinkwaterbedrijven en banken waarborgen. Deze organisaties moeten blijven functioneren, want zonder hun diensten ontstaan grote problemen.

Maar de verantwoordelijkheid reikt verder dan alleen deze organisaties. De richtlijn verplicht deze NIS2 organisaties om ook de risico's in hun toeleveringsketen te beheersen. Dit betekent dat ze maatregelen kunnen opleggen aan hun leveranciers – vaak mkb-bedrijven – om cyberrisico's te voorkomen.

Met andere woorden: jouw klanten kunnen eisen dat je laat zien dat je digitale veiligheid op orde is. Maar hoe toon je dat aan?

**WIL JE BLIJVEN WERKEN VOOR JE GROTE(RE) KLANTEN?
DAN HEB JE NIS2 QUALITY MARK NODIG.**



NIS2 Quality Mark

Om te kunnen blijven werken voor je grote klanten is het belangrijk dat je cybersecurity aantoonbaar op orde is. Het NIS2 Quality Mark is daarvoor het perfecte hulpmiddel.

Samen Digitaal Veilig helpt je met het behalen van dit certificaat. Het platform bevat alle stappen die je moet doorlopen en alle tools die je nodig hebt, inclusief voorbeelddocumenten en ondersteuning. Met het NIS2 Quality Mark certificaat toon je aan je NIS klanten dat je veilig werkt en de nodige stappen hebt gezet op het gebied van digitale veiligheid.



- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11



Waarom NIS2 Quality Mark?

Het NIS2 Quality Mark, ontwikkeld met steun van tientallen brancheverenigingen, biedt een praktisch antwoord op de eisen van de NIS2 richtlijn. Met een flexibel normenstelsel kunnen bedrijven gepaste maatregelen nemen die passen bij hun omvang en risico.

Je kunt kiezen uit drie certificeringsniveaus: QM10, QM20 en QM30. Voor de meeste mkb-bedrijven is het QM10 Basic-certificaat voldoende.

Lever je echter software, IT-diensten of werk je in een omgeving met verhoogde risico's? Dan bieden QM20 en QM30 meer zekerheid. Samen Digitaal Veilig omvat alle drie de niveaus, zodat je eenvoudig kunt opschalen als dat nodig is.

Neem geen risico. Kies voor een Europese norm die vertrouwen biedt.



Hoe werkt het?

Het behalen van het NIS2 Quality Mark bestaat uit een aantal stappen:

De eerste stap is het documenteren van je organisatieprocedures. Dit klinkt misschien ingewikkeld, maar met onze voorbeelddocumenten en invulwebinars wordt het een stuk eenvoudiger. Vervolgens richt je je op het trainen van je medewerkers. Hiervoor is een serie van praktische trainingsvideo's beschikbaar.

Daarna is het tijd om je techniek op orde te brengen. Dit betekent dat je moet aantonen dat je IT-infrastructuur en software voldoen aan de vereiste veiligheidsnormen. In de vierde stap controleer je ook de digitale veiligheid van je eigen leveranciers.

Wanneer je deze stappen hebt doorlopen, wordt alles extern getoetst. Heb je deze toetsing succesvol afgerond? Dan ontvang je het NIS2 Quality Mark certificaat als bewijs dat je voldoet aan de eisen.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11

Via het dashboard heb je toegang tot alle informatie

Wat krijg ik bij mijn abonnement?

✓ Persoonlijke opstartsessie

Je krijgt een 1-op-1 sessie met een NIS2 supportmedewerker die je in detail uitlegt hoe het platform werkt.

✓ Invulondersteuning

In online sessies helpen we je stap voor stap om alle vragen te beantwoorden en de benodigde documentatie aan te maken.

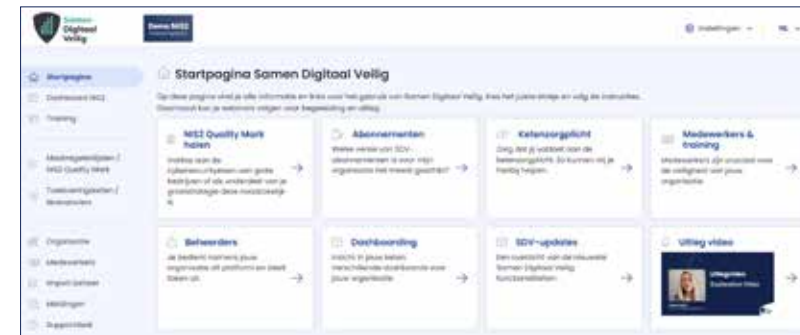
✓ Supportdesk

Heb je vragen? De supportdesk staat voor je klaar. Of het nu gaat om technische vragen, ondersteuning bij het invullen, of advies over de volgende stappen, ons team van experts begeleidt je door het hele proces.

✓ Videotraining

Om iedereen in jouw organisatie te betrekken bij de digitale veiligheid, bieden we een uitgebreide videotraining aan voor al je medewerkers.

Handig overzicht van alle vragenlijsten

A screenshot of the 'Maatregelenlijsten / NIS2 Quality Mark' page. It shows a table with the following columns: 'Naam maatregel', 'Aangemaakt', 'Voortgang maatregel', and 'Wanneer gewijzigd'. The table contains several rows of data, each with a checkbox, a name, a date, a progress bar, and another date. A sidebar on the left is visible, showing navigation options.

Toelichting en voorbeelddocumenten bij elke vraag

The screenshot displays the 'NIS2-QMIO BASIC' interface. The main content area is titled 'Beveiliging van apparaten 4.1' (Security of devices 4.1). It includes a 'Doel' (Objective) section with a shield icon, explaining that the goal is to ensure that all information processing devices are protected against unauthorized access, loss, or destruction. Below this, there are several bullet points and checkboxes detailing the requirements for device security, such as having a clear inventory of all devices and ensuring they are protected against unauthorized access.

Uitgebreide videotraining voor je medewerkers

The screenshot shows a grid of video training modules. The interface is titled 'NIS2-QMIO BASIC' and 'Training'. The grid is organized into two levels: 'Level 3' and 'Level 4'. Each module has a thumbnail image and a title. The modules in Level 3 include: 'Veilig werken op openbare wifi', 'Is werk je veilig thuis', 'De 3 beste gratis malwarebeschermers', and 'Hoe je best-in-keep goed geregeld'. The modules in Level 4 include: 'Wat als iemand op bezoek komt?', 'Schermbeschermer: zo gebruik je het veilig', 'Bewaren van documenten afgevoerd', and 'Wie je digitale sporen'. Each module has a duration indicator, such as '1 min' or '2 min'.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11

RICHTLIJNEN VOOR HET BEVEILIGEN VAN INFORMATIEBEVEILIGING

Wat is een informatiebeveiliging?

Een informatiebeveiligingsbeleid is een verzameling van informatie die beschrijft hoe informatie moet worden beschermd, het magereert hoe de informatie moet worden gebruikt en hoe informatie moet worden beschermd tegen het risico van informatiebeveiliging. Het wordt regelmatig bijgewerkt om aan te sluiten op de laatste stand van de informatiebeveiligingswetgeving.

Wat moet je doen?

- In samenwerking met de Security Officer de richtlijnen vaststellen
- De richtlijnen aan de directie presenteren
- De richtlijnen aan de medewerkers communiceren
- De richtlijnen aan de leveranciers communiceren
- De richtlijnen aan de klanten communiceren
- De richtlijnen aan de partners communiceren
- De richtlijnen aan de afdelingen communiceren
- De richtlijnen aan de werknemers communiceren
- De richtlijnen aan de vrijwilligers communiceren
- De richtlijnen aan de bezoekers communiceren
- De richtlijnen aan de leveranciers communiceren
- De richtlijnen aan de klanten communiceren
- De richtlijnen aan de partners communiceren
- De richtlijnen aan de werknemers communiceren
- De richtlijnen aan de vrijwilligers communiceren
- De richtlijnen aan de bezoekers communiceren

RICHTLIJNEN VOOR HET BEVEILIGEN VAN INFORMATIEBEVEILIGING

Informatiebeveiligingsbeleid

Zorg voor regelmatige beoordeling van informatiebeveiligingsbeleid op geplande momenten

Planstellen van vaste beoordelingsmomenten

- **Kalenderherzieningen:** Maak gebruik van vaste beoordelingsmomenten in de planning. Deze herzieningen zijn vastgesteld op basis van de planning van de organisatie.
- **Verzekeren en jaarlijkse planning:** Maak gebruik van vaste beoordelingsmomenten op basis van de jaarlijkse strategische planning.

Optie: KPI's en Metrics vaststellen

- **Key Performance Indicators (KPI's):** In het KPI's informatiebeveiligingsbeleid opgenomen om de voortgang van de informatiebeveiliging te meten.
- **Monitoring en rapportage:** Het is belangrijk om de voortgang van de informatiebeveiliging te monitoren en te rapporteren.

Documentatie en rapportage

- **Verantwoordelijkheid:** Documenteer alle beoordelingsmomenten en de resultaten van de beoordelingen.
- **Verantwoordelijkheid:** Documenteer alle beoordelingsmomenten en de resultaten van de beoordelingen.
- **Verantwoordelijkheid:** Documenteer alle beoordelingsmomenten en de resultaten van de beoordelingen.

Externe factoren

- **Wet- en regelgeving:** Als er wijzigingen zijn in de wet- en regelgeving, moet de informatiebeveiliging worden bijgewerkt.
- **Veranderingen in de organisatie:** Als er veranderingen zijn in de organisatie, moet de informatiebeveiliging worden bijgewerkt.
- **Veranderingen in de markt:** Als er veranderingen zijn in de markt, moet de informatiebeveiliging worden bijgewerkt.
- **Veranderingen in de technologie:** Als er veranderingen zijn in de technologie, moet de informatiebeveiliging worden bijgewerkt.
- **Veranderingen in de beveiligingsrisico's:** Als er veranderingen zijn in de beveiligingsrisico's, moet de informatiebeveiliging worden bijgewerkt.

INFORMATIEBEHOUD: BACK-UP BELEID

Back-up beleid

De 3-2-1 back-up systematiek

- De 3-2-1 back-up strategie is een betrouwbare manier om informatie te beschermen. Het bestaat uit drie delen:
 - **3:** Drie kopieën van de gegevens: één moet de originele kopie zijn, de andere twee moeten op andere locaties worden opgeslagen.
 - **2:** Twee verschillende media gebruiken: gebruik verschillende media voor de kopieën, zoals harde schijven en cloud opslag.
 - **1:** Een kopie op een andere locatie: zorg ervoor dat één kopie op een andere locatie wordt opgeslagen, bijvoorbeeld op een andere site of in een andere regio.

Het back-up beleid opstellen

Een back-up beleid is een document waarin de richtlijnen voor het uitvoeren van back-ups worden vastgelegd. Het moet de volgende punten behandelen:

1. **Back-upmethoden:** Beschrijving van de verschillende back-upmethoden, inclusief de frequentie van back-ups en de manier waarop de back-ups worden opgeslagen.
2. **Back-upsystemen:** Beschrijving van de verschillende back-upsystemen die worden gebruikt, inclusief de naam van het systeem, de versie en de configuratie.
3. **Beveiliging en toegangscontrole:** Beschrijving van de maatregelen die worden genomen om de back-ups te beveiligen en de toegang tot de back-ups te controleren.
4. **Verantwoordelijkheden:** Beschrijving van de verantwoordelijkheden van de medewerkers die betrokken zijn bij het uitvoeren van back-ups.
5. **Recovery Point Objective (RPO):** De maximale tijd die maximaal kan worden hersteld na een back-up.
6. **Proefrunen en testing:** Beschrijving van de manier waarop de back-ups worden getest en de manier waarop de recovery wordt getest.

OVERZICHT VAN ICT-BEDRIJFSMIDDELEN

Voorbeeld inventarislijst

Maakt gebruik van een kant-en-klare voorbeeld met een overzicht van alle ICT-bedrijfsmiddelen van een organisatie

IT Middelen	Model	Serialnummer	Locatie	Gebruiker	Aankoopdatum	Levensduur	Waar	Beveiliging
Laptop	HP EliteBook	123456789	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Server	Dell R740	987654321	Amsterdam	M. de Vries	2022-01-15	5 jaar	NL	Ja
Printer	HP LaserJet	111111111	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smartphone	Apple iPhone	222222222	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Tablet	Microsoft Surface	333333333	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smartwatch	Apple Watch	444444444	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart TV	Philips	555555555	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart speaker	Amazon Echo	666666666	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart plug	TP-Link	777777777	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart lock	Yale	888888888	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart doorbell	Ring	999999999	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart camera	Arlo	000000000	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart light	Philips Hue	111111111	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart thermostat	Nest	222222222	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart doorbell	Ring	333333333	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart camera	Arlo	444444444	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart light	Philips Hue	555555555	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart thermostat	Nest	666666666	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart doorbell	Ring	777777777	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart camera	Arlo	888888888	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart light	Philips Hue	999999999	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja
Smart thermostat	Nest	000000000	Amsterdam	J. de Vries	2023-01-15	3 jaar	NL	Ja

Ruim 100 kant-en-klare teksten en voorbeelden

Bepaal eenvoudig het risico van elke leverancier

Handig overzicht van al je leveranciers

Toeleveringsketen / leveranciers

Leveranciers spelen een belangrijke rol in de beveiliging van jouw organisatie. Deze leveranciers zijn verantwoordelijk voor de beveiliging van de ICT-gegevens die de leveranciers gebruiken.

Uitgever	Waar	Beveiliging	Actie	Aanpak	Status
ABC Truck (chemische levering)	Amsterdam	Beveiliging (Beveiliging, Beveiliging)	Beveiliging	Beveiliging	Beveiliging
Accountancy A&B & Co	Amsterdam	Beveiliging (Beveiliging, Beveiliging)	Beveiliging	Beveiliging	Beveiliging
ABC Informatie	Amsterdam	Beveiliging (Beveiliging, Beveiliging)	Beveiliging	Beveiliging	Beveiliging
Informatie Informatie	Amsterdam	Beveiliging (Beveiliging, Beveiliging)	Beveiliging	Beveiliging	Beveiliging

Risico-inventarisatie vragenlijst

Leveranciers spelen een belangrijke rol in de beveiliging van je organisatie. Het is belangrijk om de leveranciers te beoordelen op hun beveiligingsniveau. Dit kan worden gedaan door een risico-inventarisatie vragenlijst te verspreiden.

Vragenlijst voor risicobepaling

Leveranciers spelen een belangrijke rol in de beveiliging van je organisatie. Het is belangrijk om de leveranciers te beoordelen op hun beveiligingsniveau. Dit kan worden gedaan door een risico-inventarisatie vragenlijst te verspreiden.

Heeft deze leverancier digitale toegang tot informatie en/of persoonlijke gegevens van jouw organisatie of klanten?

Deze vragenlijst is bedoeld voor leveranciers die toegang hebben tot informatie en/of persoonlijke gegevens van jouw organisatie of klanten. Het is belangrijk om de leveranciers te beoordelen op hun beveiligingsniveau. Dit kan worden gedaan door een risico-inventarisatie vragenlijst te verspreiden.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11



Dit krijg je er allemaal bij

- ✓ **NIS2 Dashboard**
Krijg een duidelijk overzicht van alle vragen en antwoorden, inclusief inzicht in je voortgang en de stappen die nog nodig zijn om je volledig voor te bereiden.
- ✓ **Pre-audit webinars**
In de pre-audit begeleiden we je met een self-assessment en geven feedback, zodat je precies weet wat er nog verbeterd moet worden vóór de externe audit.
- ✓ **Importfuncties**
Maak het proces eenvoudig en efficiënt met onze importmogelijkheden. Voeg in één keer leveranciers en medewerkers toe aan het platform.
- ✓ **Supportdesk**
Stel je vragen via ons ticketsysteem en ontvang deskundige ondersteuning precies wanneer je die nodig hebt.
- ✓ **NIS2 Updates**
Blijf altijd op de hoogte van de nieuwste ontwikkelingen rondom de NIS2-richtlijn. Wij zorgen ervoor dat je niets mist.

1

2

3

4

5

6

7

8

9

10

11

Deelnemen / NIS2 QM certificaat halen?



Wil je NIS2 Quality Mark-certificering halen? Dan heb je een abonnement nodig op Samen Digitaal Veilig. Dit wordt aangeboden via partners van SDV op de Wegwijzer: <https://samendigitaalveilig.nl/wegwijzer/>

Ben je lid van een brancheorganisatie en heeft die je geattendeerd op Samen Digitaal Veilig? Dan kun je via de branchepagina gaan via de logo's op de Partnerpagina: <https://samendigitaalveilig.nl/partners/>

ALS JE LID BENT VAN EEN DEELNEMENDE BRANCHEORGANISATIE ONTVANG JE KORTING.

1

2

3

4

5

6

7

8

9

10

11

Oriëntatie, demo of vragen?

Wil je meer weten over de NIS2 richtlijn of eerst kennismaken met het NIS2 Quality Mark voordat je een besluit neemt? Wij helpen je graag op weg.

- ✓ **Volg een oriëntatiewebinar**
Ontdek wat NIS2 voor jouw organisatie betekent tijdens een van onze webinars. De data vind je op onze website.
- ✓ **Vraag een demo aan**
Benieuwd hoe het Samen Digitaal Veilig platform werkt? Neem kosteloos contact op met onze supportdesk voor een persoonlijke demo.
- ✓ **Stel je vraag**
Heb je vragen over NIS2 of het NIS2 Quality Mark? De supportdesk staat klaar om je te helpen. Dankzij de deelnemende brancheorganisaties is deze service kosteloos voor alle mkb-bedrijven.

Samen zorgen we ervoor dat je goed voorbereid bent op NIS2.



**Samen
Digitaal
Veilig**

1

2

3

4

5

6

7

8

9

10

11