



**Samen  
Digitaal  
Veilig**

# De makkelijkste oplossing voor een NIS2 veilige toeleveringsketen

Samen Digitaal Veilig is de oplossing voor NIS2 bedrijven die hun supply chain moeten controleren om te voldoen aan de NIS2 toeleveringsketeneisen.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

## De makkelijkste oplossing voor NIS2 Supply Chain Compliance

Met het NIS2 Supplychain pakket bent u verzekerd van:

- ✓ De oplossing voor NIS2-bedrijven om te voldoen aan de verplichting om de beveiliging van hun leveranciers te beoordelen.
- ✓ Gestandaardiseerd proces dat tijd en kosten bespaart.

De NIS2-richtlijn vereist een proactieve aanpak van cybersecurity, zowel binnen jouw organisatie als in de gehele supply chain. Naast het beschermen van interne IT-processen, moet je ook de beveiligingsstandaarden en risico's van leveranciers continu monitoren. Dit is de kern van de zorgplicht die NIS2 oplegt. Begin met een grondige risicoanalyse en versterk de ketenbeveiliging van jouw organisatie met een duidelijk stappenplan. Zo beschermt je cruciale processen en voldoe je aan de NIS2-eisen, terwijl je de weerbaarheid tegen cyberrisico's vergroot.





## Conformiteit met artikel 21.2d

✓ Zorgt voor naleving van de wettelijke eisen zoals gesteld in artikel 21.2d van de NIS2-richtlijn.

✓ Helpt bedrijven te voldoen aan hun verplichting om passende beveiligingsmaatregelen in de toeleveringsketen te garanderen.

Als NIS2-plichtig bedrijf draag je de verantwoordelijkheid voor de veiligheid van je eigen netwerk- en informatiesystemen én voor jouw supply chain. Artikel 21.2d vereist dat je passende technische, operationele en organisatorische maatregelen neemt om risico's te beheersen binnen de gehele keten. Door te voldoen aan de NIS2 wetgeving en jouw zorgplicht actief uit te dragen, minimaliseer je aansprakelijkheid en voorkom je boetes.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

# RISICO

## Gelaagde veiligheid die past bij het risiconiveau

✓ Risico gebaseerde benadering: leveranciers worden beoordeeld en waar nodig gecertificeerd op een niveau dat past bij hun specifieke risico.

✓ Vermijdt overbelasting van leveranciers door onnodig zware eisen. Het voorkomt dat je leveranciers te veel tijd kwijt zijn of te hoge kosten maken.

Wanneer risico's worden geïdentificeerd, moeten duidelijke afspraken met leveranciers worden gemaakt. Het gebruik van een gestandaardiseerde norm is hierbij cruciaal. Binnen Samen Digitaal Veilig werken we met het NIS2 Quality Mark – de meest haalbare en breed toegepaste oplossing voor ketenbeveiliging.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16



## Behoud van de supply chain

- ✓ Flexibele certificering voorkomt dat leveranciers afhaken door te hoge eisen.
- ✓ Helpt bedrijven hun bestaande supply chain te behouden en te versterken zonder verstoringen.

Een volledig inzicht in de beveiliging van jouw supply chain is essentieel voor effectieve samenwerking met leveranciers. Door samen te werken en inzicht te krijgen in hun beveiligingsstandaarden, verklein je niet alleen de risico's voor je eigen organisatie, maar versterkt je ook de veiligheid van de gehele keten.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

## Uitvraag bij alle leveranciers

✓ Een efficiënte uitvraag naar het beveiligingsniveau van alle leveranciers.

✓ Voorkomt handmatig werk en minimaliseert administratieve lasten.

Een eenmalige controle biedt slechts een momentopname. De NIS2-richtlijn verplicht een doorlopende evaluatie en monitoring van de beveiligingsstandaarden van jouw leveranciers. Met het NIS2 Supply chain pakket pas je de PDCA-cyclus effectief toe en houdt je jouw keten continu veilig en compliant.

Met de NIS2 Cyber Score krijgen leveranciers direct inzicht in hun beveiligingsniveau.

U kunt hen eenvoudig uitnodigen om hun score te checken – zo creëert u transparantie én versnelt u het complianceproces.

2025  
NIS2 Cyber Score



9.2

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

## Transparantie in beveiligingsniveaus

✓ Directe inzage in het beveiligingsniveau van je leveranciers.

✓ Zorgt voor een duidelijke en betrouwbare beoordeling van risico's in de keten.

Door met één standaard te werken, verminder je de complexiteit, verlaag je kosten en biedt je jouw leveranciers heldere richtlijnen. Dit zorgt voor een veerkrachtige en stabiele keten, zelfs in crisissituaties.

De NIS2 Cyber Score biedt u en uw leveranciers een eenduidige en visuele beoordeling van hun cyberweerbaarheid – essentieel voor een transparante en veilige keten.



# NIS2 wetgeving: de beveiliging van de toeleveringsketen is verplicht.

Verplicht aan de slag met je leveranciers.



**Logistieke partners**  
Transporteurs en opslagbedrijven zorgen dat je producten op tijd bij klanten komen. Een cyberaanval op hen kan dit proces verstoren.

**Financiële dienstverleners**  
Je accountant, boekhouder of payroll-provider beheert gevoelige financiële gegevens. Een hack bij hen kan eventueel leiden tot financieel misbruik.

**Productiesystemen en machines**  
Van lopende banden tot verpakkingsmachines: als deze systemen worden gehackt, kunnen productieprocessen stilvallen.

**Facilitaire leveranciers**  
Schoonmaakdiensten of beveiligingsbedrijven met fysieke toegang spelen rol in de veiligheid van je bedrijf.

**ICT-dienstverleners en software**  
Leveranciers die je netwerk, firewalls en back-ups beheren, zijn een stevig risico voor je cyberveiligheid. En ook je software is natuurlijk een risico.

**Leveranciers zoals ontwerpers of marketing- en communicatiebureaus**  
Beschermen van je ontwerpen en patënten voorkomt dat concurrenten technologie en nieuws stelen of gebruiken. Toegang tot vertrouwelijke informatie moet goed beveiligd worden om reputatieschade en verlies van concurrentievoordeel te voorkomen.

## Alle leveranciers zijn een potentieel risico

Voor je bedrijfsprocessen, je plannen, je financiële gegevens, de contracten met grote klanten. Jij bent daar zelf voor verantwoordelijk. Vraag certificering aan je leveranciers. Kijk op [www.samendigitaalveilig.nl/inkoop](http://www.samendigitaalveilig.nl/inkoop)

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16



# Handig overzicht van al je leveranciers

**Samen Digitaal Veilig** **Demo NIS2** Toeleveringsketen

Geen MFA actief Meldplicht alerts Instellingen

## Toeleveringsketen / leveranciers

Leveranciers spelen een belangrijke rol in de beveiliging van jouw organisatie. Maak hieronder je leveranciers bekend. Eerst je ICT-leveranciers daarna de andere leveranciers.

Extra ondersteuning 9 Toeleveringsketen / leveranciers

+ Toevoegen Risicoprofiel instellen Verwijderen Zoeken

<input type="checkbox"/>	Leverancier	Risico-inventarisatie	Risicoprofiel	Certificaat	Notitie	Status	Bewerk
<input type="checkbox"/>	Techl	RI bezig	Niet ingesteld			Gereed	
<input type="checkbox"/>	MF bv	RI gereed (Advies: Hoog)	Hoog			Bezig	
<input type="checkbox"/>	ASPA International	RI gereed (Advies: Hoog)	Hoog			Gereed	
<input type="checkbox"/>	GEEN RISICO	RI bezig	Geen			Bezig	
<input type="checkbox"/>	ABC Truck chemicals cleaning	RI gereed (Advies: Hoog)	Substantieel			Dringend actie	
<input type="checkbox"/>	Van de berg accountancy	RI gereed (Advies: Hoog)	Basis			Niet gestart	

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

## Bepaal eenvoudig het risico van elke leverancier

The screenshot displays the 'Samen Digitaal Veilig' NIS2 application interface. The top navigation bar includes the logo, 'Demo NIS2 Toeleveringsketen', 'Instellingen', and 'NL'. The left sidebar contains navigation options: Startpagina, Dashboard NIS2, Training, Maatregelenlijsten / NIS2 Quality Mark, **Toeleveringsketen / leveranciers**, Organisatie, Medewerkers, Import beheer, Meldingen, and Supportdesk.

The main content area is titled 'Leverancier' and 'Risico-inventarisatie vragenlijst'. It shows the supplier name 'ABC Truck chemicals cleaning' and a progress bar for 'VOORTGANG' at 100%. A blue button 'Opslaan en volgende' is visible.

**Risico-inventarisatie**  
Situatiebeschrijving  
**Vragenlijst voor risicobepaling**

Leveranciers spelen een belangrijke rol in de beveiliging van je organisatie. Hierbij gaat het niet alleen om ICT-leveranciers, maar om alle schakels in de keten die betrokken zijn bij de bedrijfsvoering, zoals productie, transport en opslag.

Voor elke leverancier dien je een risicoanalyse te maken. Op basis van de antwoorden worden de leveranciers ingedeeld in verschillende risicocategorieën.

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

Denk aan software voor financiële zaken, administratie, CRM-informatie, mailinglijsten, HR-gegevens, websites en andere software voor bijvoorbeeld planning of voorraden.

**HULPMIDDELEN**  
**EIGEN NOTITIES**  
Deze notities zijn alleen zichtbaar binnen jouw organisatie

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

## Hoe bepaal je welke leveranciers een risico vormen?

Met zoveel leveranciers is het een uitdaging om te bepalen welke een risico kunnen vormen. De NIS2-richtlijn hanteert een *All Hazards*-aanpak, wat betekent dat alle risico's van belang kunnen zijn: IT, OT, fysieke, financiële en andere risico's. Maar waar begin je, en hoe maak je de juiste keuzes?

Wij helpen je op weg! Met ons voorbeeldmateriaal en praktische checklists krijg je snel inzicht. We starten samen bij de kroonjuwelen van je bedrijf: wat moet absoluut beschermd worden? Vervolgens brengen we stap voor stap in kaart welke risico's en bijbehorende leveranciers extra aandacht verdienen.

Zo maak je een slimme en goed onderbouwde start.

**Wij ondersteunen je en hebben hiervoor een checklist**

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16



Via het dashboard heb je toegang tot alle informatie

**Samen Digitaal Veilig** Demo NIS2 Toeleveringsketen Instellingen NL

### Startpagina Samen Digitaal Veilig

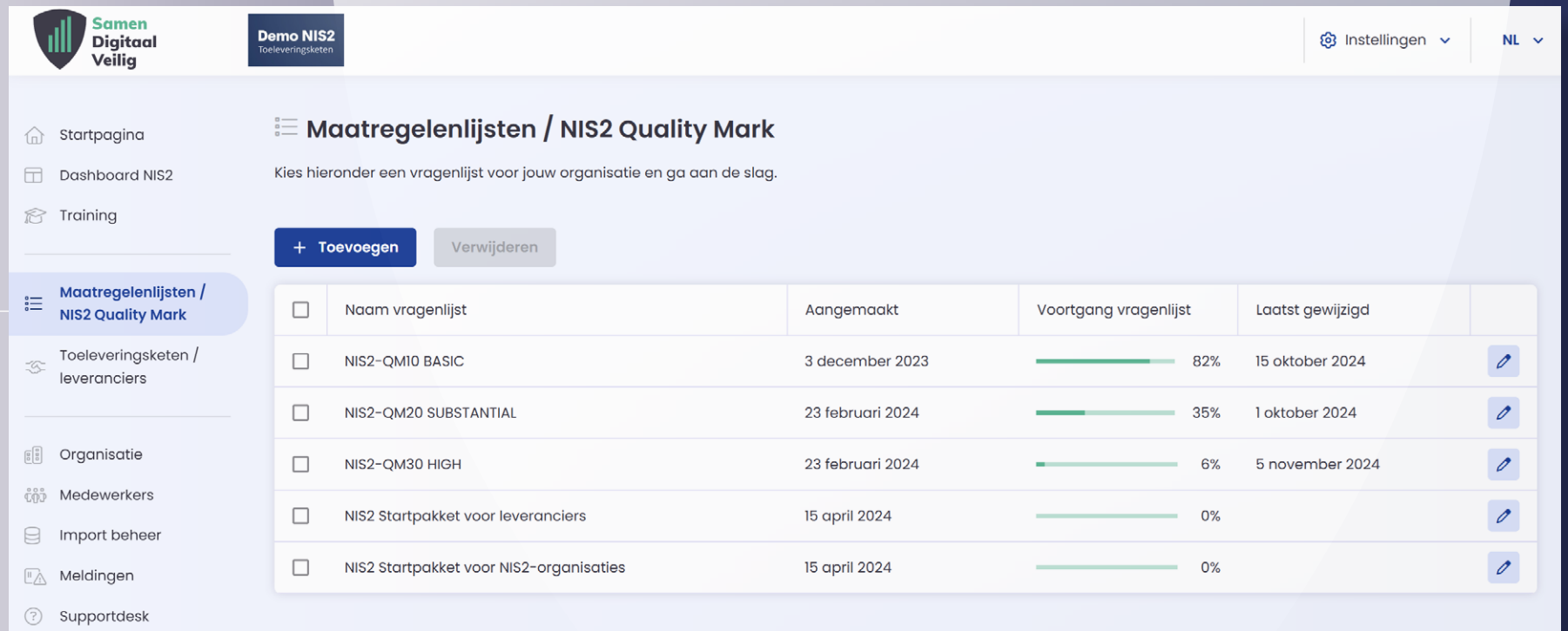
Op deze pagina vind je alle informatie en links voor het gebruik van Samen Digitaal Veilig. Kies het juiste blokje en volg de instructies. Daarnaast kun je webinars volgen voor begeleiding en uitleg.

- NIS2 Quality Mark halen**  
Voldoe aan de cybersecurityeisen van grote bedrijven of als onderdeel van je groeistrategie deze noodzakelijk is.
- Abonnementen**  
Welke versie van SDV-abonnementen is voor mijn organisatie het meest geschikt?
- Ketenzorgplicht**  
Zorg dat jij voldoet aan de ketenzorgplicht. Zo kunnen wij je hierbij helpen.
- Medewerkers & training**  
Medewerkers zijn cruciaal voor de veiligheid van jouw organisatie.
- Beheerders**  
Je bedient namens jouw organisatie dit platform en deelt taken uit.
- Dashboarding**  
Inzicht in jouw keten. Verschillende dashboards voor jouw organisatie.
- SDV-updates**  
Een overzicht van de nieuwste Samen Digitaal Veilig functionaliteiten.
- Uitleg video**  
Uitlegvideo Explanation Video






Startpagina  
Dashboard NIS2  
Training  
Maatregelenlijsten / NIS2 Quality Mark  
Toeleveringsketen / leveranciers  
Organisatie  
Medewerkers  
Import beheer  
Meldingen  
Supportdesk

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16

## Handig overzicht van alle vragenlijsten



The screenshot shows a web application interface for 'Samen Digitaal Veilig' (SDV) with a 'Demo NIS2' environment. The main heading is 'Maatregelenlijsten / NIS2 Quality Mark'. Below the heading, there are two buttons: '+ Toevoegen' (Add) and 'Verwijderen' (Remove). The main content is a table listing various questionnaires with their creation dates, progress percentages, and last update dates. Each row includes a checkbox, a name, a date, a progress bar with a percentage, a date, and an edit icon.

<input type="checkbox"/>	Naam vragenlijst	Aangemaakt	Voortgang vragenlijst	Laatst gewijzigd	
<input type="checkbox"/>	NIS2-QM10 BASIC	3 december 2023	<div style="width: 82%;"></div> 82%	15 oktober 2024	
<input type="checkbox"/>	NIS2-QM20 SUBSTANTIAL	23 februari 2024	<div style="width: 35%;"></div> 35%	1 oktober 2024	
<input type="checkbox"/>	NIS2-QM30 HIGH	23 februari 2024	<div style="width: 6%;"></div> 6%	5 november 2024	
<input type="checkbox"/>	NIS2 Startpakket voor leveranciers	15 april 2024	<div style="width: 0%;"></div> 0%		
<input type="checkbox"/>	NIS2 Startpakket voor NIS2-organisaties	15 april 2024	<div style="width: 0%;"></div> 0%		

- Startpagina
- Dashboard NIS2
- Training
- Maatregelenlijsten / NIS2 Quality Mark**
- Toeleveringsketen / leveranciers
- Organisatie
- Medewerkers
- Import beheer
- Meldingen
- Supportdesk

← Maatregelenlijsten / NIS2 Quality Mark

## NIS2-QM10 BASIC

Overzicht antwoorden

VOORTGANG  82%

### Organisatorische beheersmaatregelen

### Mensgerichte beheersmaatregelen

### Fysieke beheersmaatregelen

### Technologische beheersmaatregelen

#### Beveiliging van apparaten 4.1

- Malware voorkomen 4.4
- Back-ups en herstel 4.5
- Software updaten 4.7
- Authenticatie 4.10

## Beveiliging van apparaten 4.1

Beveiliging en beheer gebruikersapparaten

Opslaan en volgende

Bedrijfsapparaten die medewerkers en inhuurkrachten gebruiken (zoals PC's, laptops, telefoons en tablets) dienen te worden beveiligd tegen onbevoegd gebruik, het onbevoegd installeren van software en het onbevoegd wijzigen van beveiligingsinstellingen.

### Cybersecurityverzekering vereiste:

Voor bedrijven die in aanmerking willen komen voor een cybersecurityverzekering, is het van belang om **een wachtwoordbeleid te hanteren met minimaal 8 tekens** waaronder een letter, cijfer, hoofdletter en een bijzonder teken.

### Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat een gebruikersapparaat onvoldoende beveiligd is, of doordat het bedrijfsnetwerk onvoldoende beveiligd is tegen onveilige gebruikersapparaten.

In de toelichtingsdocumenten vind je voorbeelden van maatregelen die je kunt nemen en van regels die je kunt opstellen.

### HULPMIDDELEN

- Toelichtingsdoc1\_ Wat zijn gebruikersapparaten
- Toelichtingsdoc2\_ Voorbeelden technische veiligheidsmaatregelen
- Toelichtingsdoc3\_ Voorbeelden betrekken gebruikers

### EIGEN NOTITIES

Deze notities zijn alleen zichtbaar binnen jouw organisatie

### Heeft de organisatie een duidelijke inventaris van alle gebruikersapparaten en worden de beveiligingsconfiguraties van deze apparaten actief beheerd

Om een veilige digitale werkomgeving te garanderen, heb je een actueel overzicht nodig van alle gebruikersapparaten binnen een organisatie.

### ANTWOORDEN

- Ja, we hebben een volledige inventaris en beheren de beveiligingsconfiguraties van elk apparaat actief

Toelichting en voorbeelddocumenten bij elke vraag

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15**
- 16

## GAP NIS2 met ISO27001

- ✓ Registratieplicht
- ✓ Meldplicht
- ✓ Opleiding directie
- ✓ Strategisch plan inclusief handtekening directie
- ✓ Onder toezicht van een toezichthouder (vanuit de overheid dus)
- ✓ De leveringsketen is veel zwaarder qua controle en compliance voor jullie (zorgplicht)



**Er zijn ook 15 (ook technische) verschillen met ISO 27001**



**Met Samen Digitaal Veilig  
voldoet u efficiënt en betrouwbaar  
aan de zorgplicht eis, zonder  
onnodige complexiteit.**

**Vraag onze demo aan**