



**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 Corporate Supply Chain 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 Supply Chain – 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.

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 Corporate Supply Chain pakket pas je de PDCA-cyclus effectief toe en houdt je jouw keten continu veilig en compliant.



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.



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

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

Handig overzicht van al je leveranciers

portal.samendigitaalveilig.nl/?#organisatie-beheer/leveranciers

Samen Digitaal Veilig

Demo NIS2
toeleveranciers

MFA actief | Instellingen | NL

Toeleveranciers/ relaties

Leveranciers/ relaties kunnen van belang zijn voor de beveiliging van jouw organisatie.
Hieronder kun je ze invullen.

Ondersteunende documenten 6 Toeleveranciers/ relaties

+ Toevoegen | Risicoprofiel instellen | Uitnodigen (0) | Herinneren (0) | Verwijderen

Zoeken

☐	Leverancier	Risico-inventarisatie	Risicoprofiel	NIS2 Cyber Score	Certificaat	Notitie	Status	Bewerk
☐	PWS support	RI bezig	Niet ingesteld	Uitnodigen			Bezig	
☐	Adviesbureau DEF	RI bezig	Niet ingesteld	Uitnodigen			Bezig	
☐	ZX Accountancy	RI nog doen	Niet ingesteld	Uitnodigen			Bezig	
☐	International Trades	RI nog doen	Niet ingesteld	Uitnodigen			Dringend actie	
☐	TECH	RI nog doen	Niet ingesteld	Uitnodigen			Gereed	
☐	ABC toeleveringen	RI gereed (Advies: Hoog)	Niet ingesteld	Uitnodigen			Dringend actie	

© 2026 | Samen Digitaal Veilig | Disclaimer | Privacy | Algemene voorwaarden

Bepaal eenvoudig het risico van elke leverancier

portal.samendigitaalveilig.nl/?#/organisatie-beheer/leveranciers/5636/risicoanalyse/11935/beantwoorden/38

Samen Digitaal Veilig

Startpagina
Dashboard
Training
NIS2 Cyber Score
Maatregelenlijsten / NIS2 Supply Chain
Toeleveranciers/relaties
Gekoppelde organisaties
Organisatie
Medewerkers
Import beheer
Meldingen
Supportdesk

Demo NIS2
Toeleverancierslijsten

MFA actief
Instellingen
NL

← Leverancier

Risico-inventarisatie vragenlijst

LEVERANCIER
PWS support

VOORTGANG
0%

▼ Risico-inventarisatie
Situatiebeschrijving

Vragenlijst voor risicobepaling

Situatiebeschrijving

Opslaan en volgende

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.

Beschrijf wat desbetreffende leverancier voor jullie organisatie doet:

Graag vastleggen wat de leverancier doet zodat een auditor zich een beeld kan vormen van het soort leverancier, het soort bedrijf, de activiteiten, de producten en of diensten, de aard van de samenwerking en andere facetten die van belang zijn voor deze risicoanalyse.

Voorbeeld/ toelichting: Deze leverancier verzorgt onze ERP-software waar ons hele bedrijf op draait of deze leverancier doet onze boekhouding en de salarisadministratie. Tevens helpt men bij issues met facturatie. Of: de producten van de leveranciers zijn heel belangrijk voor onze eigen eindproducten die we verkopen.

HULPMIDDELEN

EIGEN NOTITIES

Deze notities zijn alleen zichtbaar binnen jouw organisatie

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 álle 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



ALL HAZARD

Voorbeelden van risico's in de keten

Voorbeelden van toeleveringsketenrisico's:

- Machineleverancier: hack vertraagt vervangingsproces
- Installatiebedrijf: planning en communicatie operationele vertragingen.
- Freight broker: ransomware-gijzeling leidt tot vertragingen in transport.
- Personeelsleverancier voor banken: lekt persoonsgegevens.
- Serviceprovider: pinterminals geblokkeerd in productie en leveringen.
- Chemische bedrijven: software werkt niet of SaaS software leverancier: uitgeverij kan niet leveren.
- Schoonmaakbedrijf: medewerker creëert een veiligheidsrisico bij het schoonmaken van de transporten.
- Transportbedrijf: risicovolle situatie bij het vervoer van vervangbare transporten.
- Architect: bouwplannen gehackt, vertraagt productie en leveringen.
- Distributiecentrum: opslag en overslag van producten en leveringen.
- Ziekenhuis wasserij gehackt: geen hygiëne in productie en leveringen.
- Trustkantoor: klantdata wordt als chantage gebruikt.
- Clearing house: ligt enkele uren stil door een aanval.
- Installateurs HVAC-systemen: zorginstellingen worden getroffen door infecties.
- Opslag chemicaliën: levensgevaarlijke situatie voor leverancier: hack verstoort productie en leveringen.
- Directe leverancier: kunnen hun werk niet doen door een cyberaanval.
- Analisten: kunnen hun werk niet doen door een cyberaanval.
- Leverancier van ziekenhuisdeuren: deuren worden geblokkeerd door een hack.
- Al-bedrijf met planningsoftware gehackt: geen leveringen door cyberincident.
- Productiebedrijf verpakkingsmateriaal: geen leveringen door cyberincident.
- Verhuurder bedrijfspanden: getroffen door ransomware, fysieke beveiliging wordt niet meer.



HOE CONTROLEER JE GROTE LEVERANCIERS

Het is begrijpelijk dat mkb-bedrijven willen vertrouwen op grote leveranciers zoals Google en Microsoft. Deze grote leveranciers hebben hun beveiliging goed geregeld. Toch blijft het belangrijk om ervoor te zorgen dat jouw bedrijf voldoet aan de uitvoerende controles te hoeven uitvoeren. Hier zijn enkele voorbeelden van hoe je grote leveranciers kunt controleren.

1. Vertrouwen op certificeringen en rapporten

Je kunt vertrouwen op de certificeringen en auditrapporten van leveranciers. Hier zijn enkele voorbeelden van hoe je grote leveranciers kunt controleren:

- ISO 27001: een veelgebruikte standaard voor informatiebeveiliging.
- SOC 2 Type II: een rapport dat de controles van een leverancier op beschikbaarheid, verwerkingsintegriteit, vertrouwelijkheid en privacy beschrijft.

2. Service Level Agreements (SLA's)

Check de SLA's die je afsluit met deze leveranciers. Beveiligingsmaatregelen beschreven of men verwijst naar deze maatregelen.

3. Advies inwinnen

Overweeg om advies in te winnen van beveiligingsadviseurs. Beoordelen of jouw gebruik van cloud- en software veilig is.

Hoewel het dus niet altijd haalbaar is voor mkb-bedrijven om grote leveranciers te controleren, kunnen ze vertrouwen op duidelijke SLA's.

Disclaimer: Samen Digitaal Veilig neemt de grootste mogelijke zorg op zich om de informatie op deze website en/of webapplicatie van de informatie te verstrekken op en via deze website en/of webapplicatie kan worden gebruikt om informatiebeveiliging en internet bedreigingen, maar (juridisch of technisch) advies, noch als enige garantie voor internet bedreigingen. Het gebruik van deze website kan leiden tot schade van welke aard ook.



NIS2 RISICO'S IN DE KETEN AANPAKKEN

Waarom zijn bedrijven verplicht om aan leveranciers van de NIS2.

Levels in de keten



N.B. Er zijn meer levels dan de hierboven genoemde. Bedrijven van de leverancier (en ook de levels daaronder) kunnen een deel van het eerste level van hun eigen leveranciers. Je hoeft dus niet alle leveranciers te controleren. Jouw leverancier moet zijn eigen leveranciers beoordelen.

Het doel van de NIS2 wetgeving is het voorkomen van cyberaanvallen.

Het veilig maken van de keten wordt gerealiseerd door de volgende stappen:

1. Inventarisatie van risico's
2. Aankondiging van gewenste compliance naar leverancier
3. Opleggen en afspreken van een te halen norm
4. Project opvolgen en vragen naar norm
5. Inkoopvoorwaarden afstemming
6. Ontvangen van norm
7. Jaarlijks opvolgen van je leveranciers



WAAROM BASIS CYBERHYGIËNE OPLEGGEN AAN ALLE LEVERANCIERS?

Van de moderne zakelijke wereld is cybersecurity een cruciale pijler geworden. Met de toename van cyberaanvallen en datalekken is het van groot belang dat bedrijven niet alleen hun eigen systemen beveiligen, maar ook de systemen van hun leveranciers. In dit kader wordt steeds vaker een minimum aan basis cyberhygiënemaatregelen geëist van alle leveranciers. Het NIS2 QM-10 certificaat is hierbij een vaak gehanteerde standaard. Uiteraard zijn er ook andere, zwaardere cybersecuritynormen die men kan opleggen.

Het belang van cyberhygiëne

1. Naleving van regelgeving: in veel sectoren en regio's wordt cybersecurity steeds vaker gereguleerd. Het naleven van basis cyberhygiënemaatregelen helpt bedrijven om te voldoen aan wettelijke vereisten en voorkomt boetes en sancties.
2. Bescherming tegen cyberaanvallen: leveranciers vormen vaak een zwakke schakel in de keten. Een succesvolle aanval op een leverancier kan desastreuze gevolgen hebben voor het gehele netwerk. Basis cyberhygiëne helpt bij het verminderen van deze risico's door fundamentele beveiligingsmaatregelen te implementeren.
3. Kostenbesparing op de lange termijn: de financiële impact van een cyberaanval kan enorm zijn. Dit omvat niet alleen de directe kosten van herstel, maar ook de kosten van reputatieschade en juridische consequenties. Door een minimum aan basis cyberhygiëne te eisen, kunnen bedrijven deze risico's aanzienlijk verkleinen en op de lange termijn kosten besparen.
4. Vertrouwen en reputatie: bedrijven die basis cyberhygiëne opleggen aan hun leveranciers, kunnen hun reputatie versterken.
5. Integratie van cybersecurity in de keten: door basis cyberhygiëne te eisen, kunnen bedrijven de cybersecurity van de keten integreren.

Extra uitleg zodat je alles goed regelt

Het opleggen van basis cyberhygiëne

1. Standaardisering in inkoopvoorwaarden: grote bedrijven zijn al enige jaren geleden begonnen met het standaard opnemen van basis cyberhygiënemaatregelen in hun inkoopvoorwaarden.

Via het dashboard heb je toegang tot alle informatie

[Startpagina](#)

[Dashboard](#)

[Training](#)

[NIS2 Cyber Score](#)

[Maatregelenlijsten / NIS2 Supply Chain](#)

[Toeleveranciers/ relaties](#)

[Gekoppelde organisaties](#)

[Organisatie](#)

[Medewerkers](#)

[Import beheer](#)

[Meldingen](#)

[Supportdesk](#)

Demo NIS2
Toezeggingen

Toevoegen

Risicoprofiel instellen

Uitnodigen (0)

Herinneren (0)

Verwijderen

Zoeken

☐	Leverancier	Risico-inventarisatie	Risicoprofiel	NIS2 Cyber Score ^①	Certificaat	Notitie	Status	Bewerk
☐	PWS support	RI bezig	Niet ingesteld	Uitnodigen		Notitie	Bezig	Bewerk
☐	Adviesbureau DEF	RI bezig	Niet ingesteld	Uitnodigen		Notitie	Bezig	Bewerk
☐	ZX Accountancy	RI nog doen	Niet ingesteld	Uitnodigen		Notitie	Bezig	Bewerk
☐	International Trades	RI nog doen	Niet ingesteld	Uitnodigen		Notitie	Dringend actie	Bewerk
☐	TECH	RI nog doen	Niet ingesteld	Uitnodigen		Notitie	Gereed	Bewerk
☐	ABC toeleveringen	RI gereed (Advies: Hoog)	Niet ingesteld	Uitnodigen		Notitie	Dringend actie	Bewerk

Ondersteunende documenten

6 Toeleveranciers/ relaties

© 2026 | Samen Digitaal Veilig | Disclaimer | Privacy | Algemene voorwaarden

Handig overzicht van alle vragenlijsten

portal.samendigitaalveilig.nl/?#/organisatie-beheer/vragenlijsten

Demo NIS2 Toeleveringsketen

MFA actief Instellingen NL

Maatregelenlijsten / NIS2 Supply Chain

Kies hieronder een vragenlijst voor jouw organisatie en ga aan de slag.

+ Toevoegen Verwijderen

☐	Naam vragenlijst	Aangemaakt	Voortgang vragenlijst	Laatst gewijzigd	
☐	NIS2-SC10 BASIC	29 april 2025	49%	18 november 2025	

© 2026 | Samen Digitaal Veilig | Disclaimer | Privacy | Algemene voorwaarden

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