

WEBINAR · CYBERBEVEILIGINGSWET (NIS2)

Welkom

Grip op digitale veiligheid voor jouw organisatie

Van der Hoff ICT in samenwerking met **Samen Digitaal Veilig**

Waar gaan we het over hebben?

Het programma van vandaag en onze rol als jouw ICT-partner.

- 1 Introductie Samen Digitaal Veilig
- 2 Voor wie geldt de wet – direct & indirect
- 3 Welke gevolgen heeft dit voor jou?
- 4 Wat moet je doen?
- 5 Zo helpen Van der Hoff ICT & SDV
- 6 Q&A

ONZE ROL ALS JOUW MSP

-  Informeren over je (bestuurlijke) verantwoordelijkheden
-  Adviseren over passende maatregelen en dienstverlening
-  Beveiligen en de continuïteit van kritieke systemen borgen
-  Ondersteunen bij incidenten en de wettelijke meldplicht

Voordat we starten

Een paar huishoudelijke mededelingen.

 Dit webinar wordt opgenomen

 Alle camera's staan uit

 Microfoons staan op mute

 Stel je vragen via de chat (bovenin je scherm)

 Slides en opname worden na afloop toegestuurd

The background image shows a person's hands typing on a laptop keyboard. Overlaid on this are several digital security-themed elements: a large white shield with a padlock icon, two input fields labeled 'USER NAME' and a password field with asterisks, and a network of glowing blue lines and nodes. The text is enclosed in a white bracket-like shape.

“U hoeft niet NIS2-plichtig te zijn om tóch geraakt te worden door de Cyberbeveiligingswet.”

“Een cyberincident stopt zelden bij het bedrijf waar de hacker binnenkomt.”

“De Cyberbeveiligingswet verandert de spelregels in de hele keten. Grote klanten gaan steeds vaker aan hun leveranciers vragen: hoe goed bent u digitaal beveiligd?”



NIS2 Cyberbeveiligingswet

Een wet met grote gevolgen

Startdatum
15-8-2026



Samen Digitaal Veilig

SDV is het grootste NIS2-platform van Nederland.

- Opgezet voor en door > 105 samenwerkende brancheorganisaties om ruim 220.000 bedrijven en organisaties te ondersteunen bij deze nieuwe wet
- > 200 aangesloten kennispartners (M(S)SP's, Consultants, Accountants, Advocaten, Banken, Verzekeraars)

2 doelstellingen:

- **NIS2 'zacht laten landen voor het mkb'**
- **Geen disruptie in de supply chain**

NIS2 'plichten'



Registratieplicht



Meldplicht



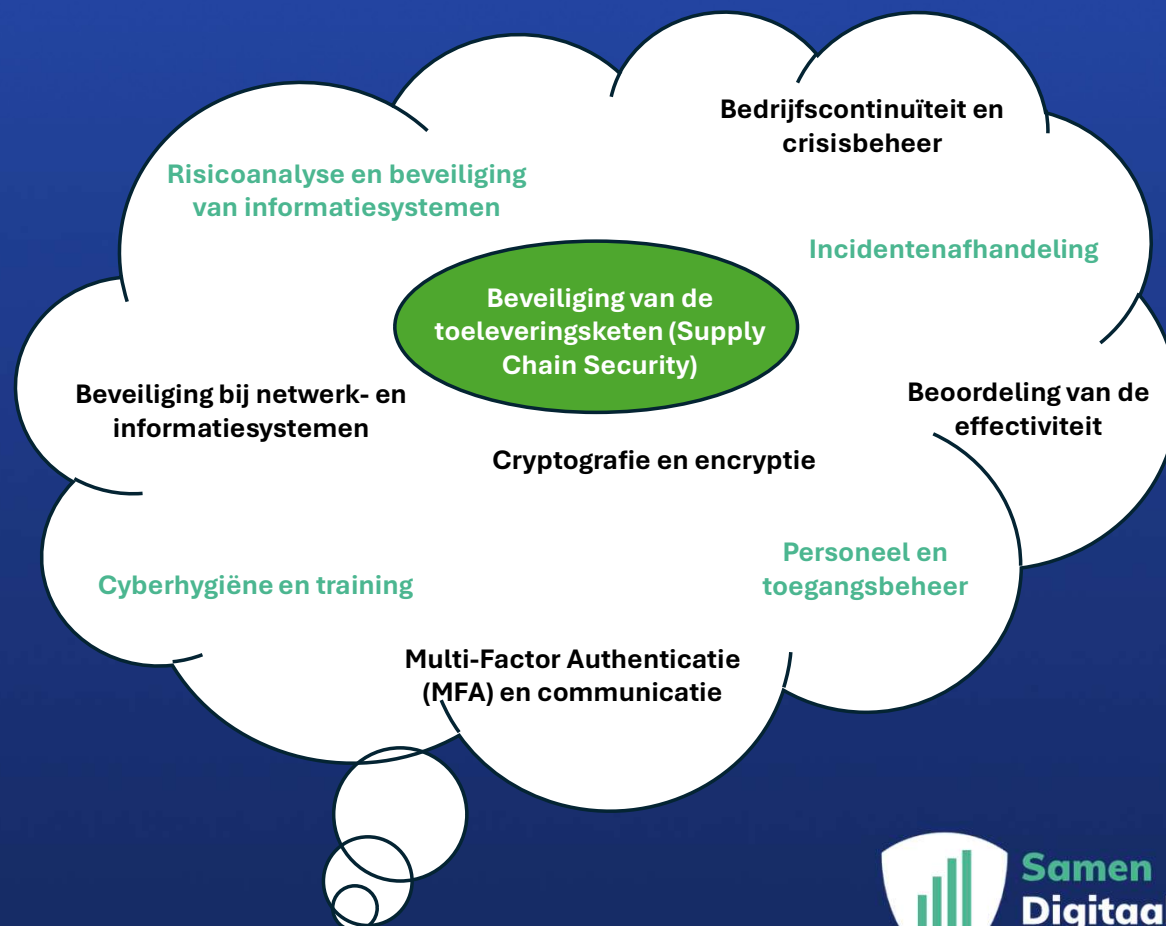
Toezicht



Zorgplicht



Bestuurders
aansprakelijkheid



Belangrijk

Registratieplicht

- Verplichte registratie
 - Mijn.ncsc.nl
1. Organisatiegegevens
 2. Aanvullende organisatiegegevens
 3. Contactgegevens
 4. Netwerkgegevens
 5. Samenvatting en versturen

Meldplicht -> mijn.ncsc.nl

Vroegtijdige waarschuwing binnen 24 uur. Je geeft aan of het incident vermoedelijk kwaadwillig is en of er gevolgen zijn over de grens. Ook deel je de contactgegevens van je contactpersoon.

Melding binnen 72 uur. Je werkt je eerste waarschuwing bij en geeft een eerste beoordeling van de ernst en de gevolgen. Heb je indicatoren van aantasting? Deel die dan ook.

Eindverslag binnen 1 maand na je melding. Je beschrijft het incident, de oorzaak en de maatregelen die je nam.

Note: Incident in de toeleveringsketen: meld dit bij voorkeur bij het NCSC of AP (bij persoonsgegevens) e/o bij je IT partner, maar kijk ook of er iets over staat in het (nieuwe) contract met je (grote) klant(en)



NIS2 en alle bedrijven in de keten

Uitdaging

Ruim 100.000 leveranciers van NIS2 bedrijven moeten aantoonbaar bewijzen dat ze veilig digitaal werken -> *“Passend & evenredig”*

Essentiële organisaties

Belangrijke organisaties

Ca. 10.000 NIS2 bedrijven



Bedrijven die leveren aan NIS2 bedrijven

50.000 leveranciers

De toeleverancier van de toeleverancier

83.500 leveranciers



Samen
Digitaal
Veilig

Wat zegt de Toezichthouder?



Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en
Klimaat

Home > Onderwerpen > 5. Digitale weerbaarheid > Cyberbeveiligingswet

Toeleveringsketen en cyberbeveiliging

Welke risico's voor de cyberbeveiliging brengen uw leveranciers en hun onderaannemers met zich mee voor uw organisatie? Valt uw organisatie onder de Cyberbeveiligingswet (Cbw), dan moet u aan de slag met deze vraag.

De beveiliging van uw toeleveringsketen is niet alleen relevant vanuit bedrijfseconomisch perspectief, maar ook vanuit veiligheidsperspectief. Door de keten goed te beschermen, voorkomt u verstoringen en zorgt u voor een stabiele bedrijfsvoering. Dit draagt niet alleen bij aan de continuïteit van uw eigen organisatie, maar biedt ook stabiliteit aan de hele samenleving.

Governance inrichten voor ketenbeveiliging

Ketenbeveiliging gaat over het beschermen van zowel bestaande als nieuwe leveranciers van uw organisatie. Hierbij kunt u het beste zo vroeg mogelijk cybersecurity- en cyberweerbaarheidsexperts betrekken. Maar digitale veiligheid is niet alleen een verantwoordelijkheid van een cybersecurity-afdeling. Het is een gezamenlijke inspanning van de hele organisatie. Van alle afdelingen, zoals financiën, juridische zaken, inkoop en HR. Samen kunnen zij goed meewegen welke afhankelijkheden en risico's er zijn.

Het bestuurlijk inrichten van afspraken, verantwoordelijkheden en processen (governance) voor ketenbeveiliging valt onder de bestuurlijke verantwoordelijkheid.

Risicoanalyse van processen en leveranciers

Met behulp van een risicoanalyse bepaalt u van uw huidige leveranciers hoe groot de impact is op uw eigen organisatie, als ze bijvoorbeeld wegvallen of worden gehackt. Welke processen en data hebben met leveranciers te maken? Welke risico's en afhankelijkheden zijn er? Zo identificeert u uw kritieke leveranciers met hun risico's.

Gesprekken en schriftelijke afspraken met leveranciers

U wilt de risico's van uw leveranciers beheersen. Dan kunt u het beste een gesprek voeren met deze leveranciers over elkaars afhankelijkheden en cyberbeveiliging. Bekijk samen waar de veiligheid beter kan en maak een plan om dit te verbeteren.

Met de leveranciers die een grote impact hebben op uw organisatie, kunt u schriftelijke afspraken maken. Deze zorgen voor duidelijkheid en een betere controle op de veiligheid binnen de hele keten.

Monitoring van afspraken

Het opzetten van een systeem helpt u om te controleren of uw leveranciers zich aan de gemaakte beveiligingsafspraken houden. Ook moet u ervoor zorgen dat deze afspraken up-to-date blijven en regelmatig worden getoetst, bijvoorbeeld met assessments of audits.

Gevolgen Cbw voor leveranciers

Leveranciers aan organisaties die onder de Cbw vallen, zullen indirect de gevolgen van de wet merken. Zo is de verwachting dat Cbw-organisaties aan hun leveranciers om extra maatregelen zullen vragen, zoals het hebben van bepaalde certificaten. Volgens de wet zijn de Cbw-organisaties immers verantwoordelijk voor voldoende beveiliging van de toeleveringsketen.



Samen
Digitaal
Veilig



Wat moeten jullie doen?

Haal NIS2-Certificering door cybersecurity maatregelen te nemen. Organisatorisch, medewerkers, fysiek en technisch.

Hoe regel je dat? Zorg dat er 1-2 medewerkers mee starten. Maak een team. Geef steun vanuit de directie.



Deze wetgeving heeft een domino-effect

Bij elke nieuwe wet zijn er effecten.

Algemene inkoopvoorwaarden



Veilig samenwerken
in de keten

Artikel 1

De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier.

Artikel 2

De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier.

Artikel 3

De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier.

Artikel 4

De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier.

De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier.

Artikel 5

De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier.

Artikel 6

De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier.

Artikel 7

De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier.

Artikel 8

De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier.

Artikel 9

De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier.

Artikel 10

De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier.

Artikel 11

De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier. De afnemer aanvaardt de inkoopvoorwaarden van de leverancier.

Samen Digitaal Veilig is een initiatief van



VNO-NCW

Inkoopvoorwaarden met cybersecurity verplichting wordt de standaard.

Dus als je levert aan of samenwerkt met een NIS2 organisatie of je levert aan een bedrijf dat levert aan een NIS2 organisatie. In al die gevallen wordt NIS2 certificering een 'licence to operate'.



Samen
Digitaal
Veilig



Neem je 3 grootste klanten in gedachten

**Die mailen: “we ontvangen graag het bewijs dat je
Cybersecurity op orde is”**

Kun je dat vandaag?



**Samen
Digitaal
Veilig**



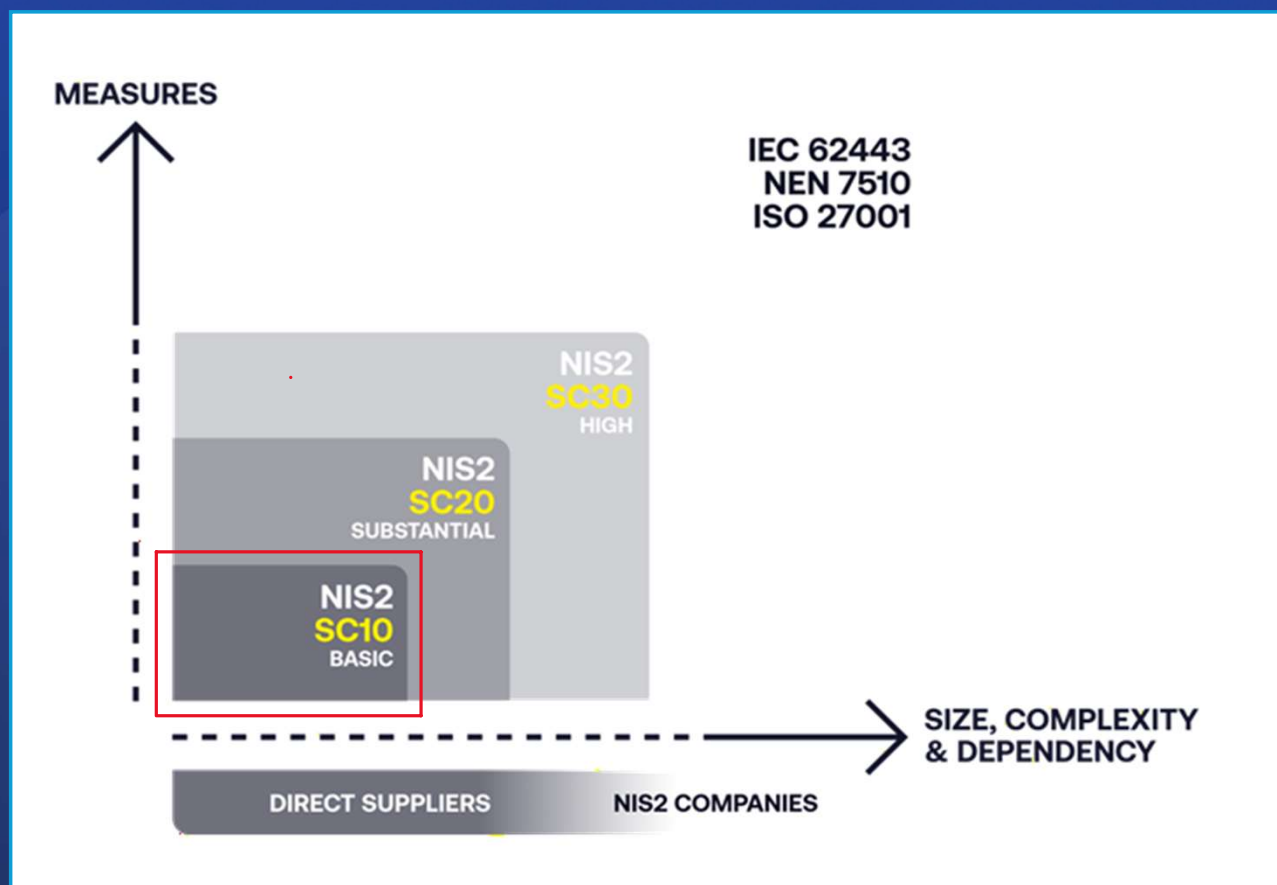
NIS2-certificering is je digitale brandblusser

“Het zal wel even wennen zijn voor bedrijven maar het hebben van NIS2-Certificering wordt vanaf Q3 2026 de standaard. Je license to operate!”

Een cyberincident lijkt op een brand: het verspreidt zich snel en kan je bedrijf in één dag verwoesten. Net zoals investeren in rookmelders en brandblussers moet dat nu in cybersecurity certificering.



De norm voor de toeleveringsketen



NIS2-SC10 (Basic)

NIS2-SC20 (Substantial)

NIS2-SC30 (High)

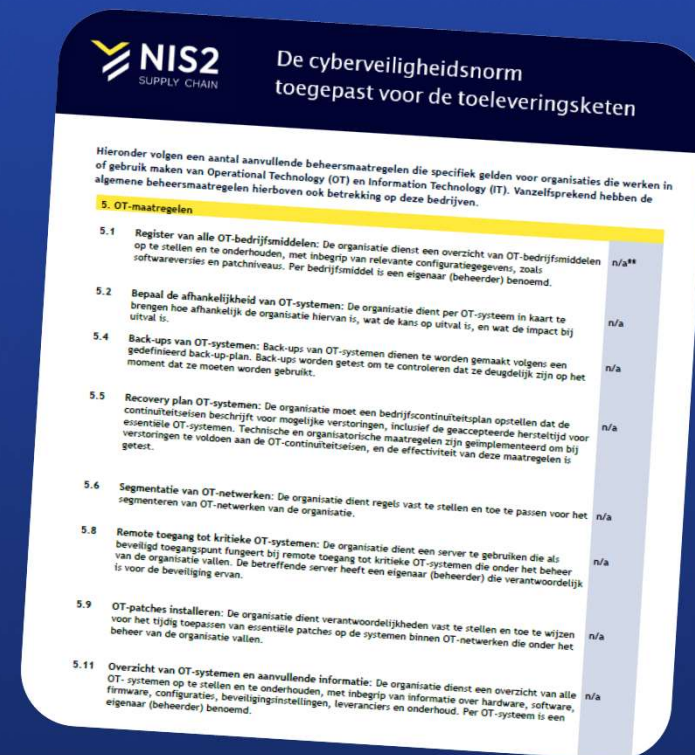


ISO27001 vs NIS2

Q: Ben je met ISO27001 ook 'Compliant' met NIS2?

Antwoord is NEE

Maatregelen	NIS2	ISO27001
Registratieplicht (NCSC)	✓	✗
Onder toezicht van een Toezichthouder	✓	✗
Bestuurlijke aansprakelijkheid & Boetes	✓	✗
Meldplicht procedures	✓	✗
Opleiding directie (verplicht)	✓	✗
Strategisch cybersecurityplan (door directie goedgekeurd & ondertekent)	✓	✗
Verplichte zorgplicht toeleveranciers (strengere eisen)	✓	✗
OT (Operational Technology) Security	✓	✗
IT-maatregelen, w.o.:	✓	✗
Actueel houden van programmacode en externe componenten	✓	✗
Procedures voor software deployement		
Overzicht van geleverde software		
Afstemming met klanten over updates		



Hoe kun je NIS2- certificering halen?

Cybersecurity maatregelen nemen en vastleggen. Het is wel wat werk maar de meeste bedrijven en organisaties hebben de technische zaken al deels geregeld. Het gaat dus vooral om zaken op papier zetten en medewerkers trainen als voorbereiding op een audit.



CERTIFICATE

European Supply Chain Cyber Security Standard



NIS2
SUPPLY CHAIN

NIS2-SC10
BASIC

The audit was performed by:
Audit Company

Valid from 28-08-2024 until 27-08-2027

NIS2 Supply Chain certificate:

Company ABC

for completing the NIS2 Supply Chain Audit successfully

Dr. D.P. Noordhoek RAE

Director-Secretary

Foundation for Quality & Innovation



#2738491039



**Samen
Digitaal
Veilig**

Je cyber op orde

Het is wel wat werk maar daarna hebt de aantoonbaar bewijs dat je cybersecurity op orde is. Goed voor je eigen veiligheid, je imago en je humeur.



Samen Digitaal Veilig platform



Alle stappen kant en klaar uitgewerkt incl. voorbeelden om het NIS2 Supply Chain certificaat te halen.

- ✓ Alle onderdelen in lijsten (de hele NIS2 compleet van A-Z)
- ✓ Begrijpelijke taal
- ✓ Inclusief voorbeelddocumenten (knippen en plakken)
- ✓ Leveranciers risico management tool



Welke stappen doorloopt een end-user?

Van onboarding tm certificering!

Continu proces!

1 Activatie



- ✓ Toegang tot platform

2 Onboarding & Opleiding



Planning voor onboarding sessie:

3 Begeleiding via webinars



- Inplannen (landelijke) sessie(s):
- ✓ maatregelenlijsten *
 - ✓ Leveranciers activatie (keten)
 - ✓ Pre-Audit

4 Auditfase



Audit door erkende partij

5 Certificering



- Ontvangst NIS2 SC-Certificaat
- ✓ Tbv. oa. klanten, inkopers, verzekeraars

** Technologische e/o Awareness maatregelen afstemmen met Van der Hoff ICT*



Demo



**Samen
Digitaal
Veilig**

Stel jezelf de vraag:

Ga ik het risico nemen om mogelijk klanten te verliezen, nieuwe opdrachten te missen? Of ga ik aan de slag?



Key take aways:

- De Cbw is in werking 15 Augustus 2026
- De gehele keten moet veilig(er) werken, conform het risico dat je loopt als toeleverancier
- De basis op orde is 'de fundering'
- Wacht niet (langer) af: Start nu met je eigen NIS2-SC traject en blijf onderdeel van de (toeleverings)keten
- Van der Hoff ICT & SDV ondersteunen





van der Hoff
ICT

Wij gaan je helpen!



Samen
Digitaal
Veilig

Groepsdeal



Waarom het slim is om nú de logische stap te zetten.

In 2026 (hoogstwaarschijnlijk 1 juli) treedt de Europese NIS2 in Nederland in werking onder de naam Cyberbeveiligingswet. Grote bedrijven en organisaties – naar schatting 8.500 – vallen direct onder de wet en zijn verplicht al hun leveranciers te controleren op digitale veiligheid.

Dat betekent dat, in de supply chain, 60.000 – 100.000 mkb-bedrijven aantoonbaar moeten maken dat hun cyberbeveiliging op orde is.

Voor jouw bedrijf betekent dit één ding: zonder bewijs van goede cyberbeveiliging loop je risico's. Het enige logische acceptabele bewijs is certificering.

De eenvoudigste en meest haalbare route voor mkb-bedrijven is het halen van NIS2 Supply Chain certificering.



De oplossing: Groepsdeal NIS2 Supply Chain

Met de Groepsdeal regel je alles in één keer.

Wat zit erin?

- SDV-abonnement (incl. NIS2 SC-registratie)**
 - Toegang tot het Samen Digitaal Veilig platform met alle te nemen maatregelen, tools, voorbeeldtemplates en begeleiding.
 - Officiële registratie in het NIS2 transparanteregister (2026).
 - Deelneme aan de pre-audittraining, zodat je precies weet wat je kunt verwachten.
- Audit (toetsing) & certificaat**
 - Gegarandeerde auditplanning via onze groepsafspraken.
 - Onafhankelijke toetsing of het papierwerk compleet is en de antwoorden kloppen via een gesprek (online en/of op locatie).
 - Je ontvangt het NIS2 SC-certificaat na een positieve toets.

Voordelen Groepsdeal

- De auditprijs is eenmalig. Een NIS2-certificaat is 3 jaar geldig.
- Extra korting op de prijs voor licenties en audit.
- Je audit wordt gegarandeerd ingepland.
- Je voorkomt klantverlies en laat zien dat je veilig werkt.
- Je kunt kiezen uit 3 niveaus, afhankelijk van de eisen van je klanten:

NIS2-SC10 Basic (geschikt voor 70% van de bedrijven en organisaties)
NIS2-SC20 Substantial (voor bedrijven die veel digitaal werken)
NIS2-SC30 High (voor bedrijven met meer risico)

De Groepsdeal: verzekerd van tijdige certificering

Het duurt een paar maanden om auditproof te worden. (Langer voor SC20- en SC30). De meeste bedrijven willen voor de zomer van 2026 klaar zijn. Maar er is een groot probleem: auditoren schaars. Momenteel zijn er te weinig auditoren beschikbaar om iedereen op tijd te helpen. Alleen bedrijven die zich nu aanmelden voor de groepsdeal krijgen gegarandeerd voorrang.

Met de Groepsdeal voorkom je klantverlies, borg je je continuïteit en laat je zien dat jouw bedrijf klaar is voor de toekomst.

>> Groepsdeals worden aangeboden via partners van Samen Digitaal Veilig.

Bestel nu om zeker te zijn van deelname.



Samen werken we aan je digitale weerbaarheid

De Groepsdeal – nog te gebruiken tot en met 30 september 2026.

DE GROEPSDEAL · PROFITEER TOT EN MET 30 SEPTEMBER 2026



Lager maandbedrag

Een voordelig tarief voor het Samen Digitaal Veilig platform.



Auditplanning in 2026

Gegarandeerd een plek in de auditplanning van dit jaar.



Technische dienstverlening

De ondersteuning en expertise van Van der Hoff ICT.

Denk na over je belangrijkste risico's en welke vervolgstappen je wilt zetten. Wij gaan er graag met je over in gesprek.

TOT SLOT

Vragen of meer informatie?

Neem gerust contact op met ons verkoopteam. We denken graag met je mee.

 **0485 782 380**

 **verkoop@vanderhoffict.nl**

 **www.vanderhoffict.nl**

Van der Hoff ICT · Transportcentrum 3, 5835 CT Beugen