

Cyberveiligheid in de Zorg

NIS2 en de Verantwoordelijkheid van Inkopers

nevi Zorgcongres





Even voorstellen...



Ron Vermeulen
Manager Partners
Samen Digitaal Veilig



V N O N C W



Samen Digitaal Veilig

SDV is het **grootste NIS2-platform** van Nederland. Het is opgezet voor en door meer dan **100 brancheorganisaties**. En wordt ondersteund door ruim **90 kennis- en marktpartijen**.

Samen bereiken we ruim **200.000 bedrijven** die we informeren en helpen bij deze nieuwe wet.



NIS2 voor jou ▾

Kennis ▾

Deelnemen >

Een sterke keten heeft 100% betrouwbare schakels

Mkb-bedrijven

Breng je cyberveiligheid op orde, train medewerkers, check leveranciers en laat zien dat je veilig werkt.

Verhoog je cyberveiligheid >

NIS2 organisaties

Ruim 8.000 organisaties vallen onder de NIS2 Cyberbeveiligingswet en moeten eraan voldoen.

Regel alles voor NIS2 >

NIS2 Cyber Score

Doe nu de gratis NIS2 Cyber Score-check. In 10 minuten krijg je inzicht én een handige PDF met jouw score.

Check het nu! >

Partners

Ontdek de [ruim 100 brancheorganisaties](#) en [grote bedrijven](#) die zich al aansloten bij Samen Digitaal Veilig



Laatste nieuws

Forvis Mazars rapport: Cyber security in 2026



Noodplan op papier en bedrijven moeten ook hun...



Zo gevaarlijke echt. Zo doortrapt.



Nieuwe doorverwijsboom helpt organisaties bij vragen over d...



Flink meer cyberaanvallen op productiemachines en...



Digitale veiligheid in de verkiezingsprogramma's 2025



NIS2 Cyberbeveiligingswet

Een wet met grote gevolgen

**Wie is al helemaal op de hoogte
van de NIS2-richtlijn en de
Cyberbeveiligingswet?**

NIS2

Cyberbeveiligingswet

8.000–10.000 bedrijven en organisaties vallen direct onder de wet.

Indirect krijgen 50.000 – 100.000 bedrijven en organisaties ook met de wet te maken. Ze zijn onderdeel van de "keten" en moeten kunnen bewijzen dat ze veilig digitaal werken.

NIS2 Sectoren

Sectoren bijlage I	Sectoren bijlage II
Energie	Digitale aanbieders (online marktplaatsen)
Transport	Post- en koeriersdiensten
Bankwezen	Afvalstoffenbeheer
Infrastructuur financiële markt	Levensmiddelen
Gezondheidszorg	Chemische stoffen (productie, opslag en distributie)
Drinkwater	Onderzoek (onderzoeksinstellingen)
Digitale infrastructuur	Vervaardiging / manufacturing
Beheerders van ICT-diensten (MSP's)	
Afvalwater	
Overheidsdiensten	
Lokale overheden (gemeenten)	
Ruimtevaart	

NIS2 Sector: Gezondheidszorg

Bevoegde autoriteit	Sector	Subsector	Grote organisaties	Middelgrote organisaties	Kleine- en micro-organisaties
Minister van Volksgezondheid, Welzijn en Sport	 Gezondheidszorg	Zorgverleners; laboratoria; onderzoek & ontwikkeling van geneesmiddelen; vervaardiging van farmaceutische basisproducten en -preparaten; vervaardiging van medische hulpmiddelen die van cruciaal belang zijn bij noodsituaties op het gebied van de volksgezondheid	Essentieel	Belangrijk	Niet van toepassing
		Entiteiten met een distributievergunning voor geneesmiddelen; alleen indien geïdentificeerd als kritieke aanbieder in de Critical Entities Resilience Directive (CER-richtlijn)	Essentieel	Belangrijk	Niet van toepassing

	 Werknemers		 Jaaromzet		 Balanstotaal
Grote organisaties	= > 250	of	> 50 mln	+	> 43 mln
Middelgrote organisaties	= > 50	of	> 10 mln	+	> 10 mln

**Wie kent de impact van deze wet op
de gezondheidszorg?
Kan je voorbeelden noemen?**

Impact NIS2 op de gezondheidszorg

- **Veel bredere reikwijdte in de zorg:** niet alleen ziekenhuizen, maar ook andere zorginstellingen, labs, farmaceuten en digitale zorgdiensten vallen onder de NIS2-richtlijn en moeten zich registreren (registratieplicht)
- **Verplichte risicoanalyse en incidentrespons:** zorginstellingen moeten structureel risico's identificeren en aantoonbaar maatregelen treffen om patiëntenzorg niet in gevaar te brengen (zorgplicht)
- **Verhoogde meldplicht & korte deadlines:** ernstige cyberincidenten moeten binnen 24 uur gemeld worden bij autoriteiten (meldplicht)
- **Persoonlijke verantwoordelijkheid van bestuur & directie:** Nalatigheid kan leiden tot boetes en directe aansprakelijkheid van bestuurders binnen zorgorganisaties. Verplichte trainingen voor bestuur & directie (trainingsplicht)
- **Zorgketen moet aantoonbaar veilig zijn:** leveranciers van zorginstellingen moeten óók voldoen en een aantoonbaar cyberveiligheidsniveau hebben.



Wat zegt de Toezicht houder?

De RDI zegt over Toeleveringsketen en cyberbeveiliging o.a.:



Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

De NIS2 Cyberbeveiligingswet vervangt in 2026 de huidige wet.

Dit is belangrijk omdat:

- De wet geldt voor veel méér organisaties dan voorheen.
- Bestuurders worden verantwoordelijk voor cybersecurity.
- Continuïteit en ketenveiligheid staan centraal.

Zorgplicht

Organisaties waarvoor de Cyberbeveiligingswet geldt, zijn verantwoordelijk voor goede beveiliging. U moet maatregelen nemen om te zorgen dat er geen grote problemen ontstaan.

Wat houdt de zorgplicht in?

De zorgplicht begint met het maken van een risicoanalyse. Daarmee brengt u in kaart welke dreigingen relevant zijn voor uw organisatie en welke gevolgen een incident kan hebben. Op basis daarvan kiest u maatregelen die passen bij uw situatie.

Denk bijvoorbeeld aan:

- het regelmatig updaten van software;
- het beveiligen van toegang tot systemen met sterke wachtwoorden en extra verificatie;
- het maken van duidelijke afspraken met leveranciers over cyberbeveiliging.

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

Deze wetgeving heeft een domino-effect

Bij elke nieuwe wet zijn er effecten.

2 Mkb-bedrijven kunnen verlies van grote klanten voorkomen

NIS2 verplicht duizenden grote organisaties om hun leveranciers te controleren op digitale veiligheid. Dit raakt naar schatting 50.000 – 100.000 mkb-bedrijven. Wie zijn cybersecurity niet aantoonbaar op orde heeft, loopt het risico waardevolle klanten te verliezen. Dat risico is te groot om te negeren.

3 Banken laten cybersecurity zwaarder meewegen

Steeds vaker nemen banken digitale veiligheid mee in hun risicoanalyse. Bedrijven zonder aantoonbare cybersecurity krijgen moeilijker financiering. Je cybersecurity op orde hebben zal een vast onderdeel van kredietbeoordeling worden.

9 NIS2-certificering is je digitale brandblusser

“Het zal wel even wennen zijn voor bedrijven maar het hebben van NIS2-Certificering is vanaf 2026 de standaard.”

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 aantoonbare cybersecurity.

4 Accountants letten scherper op digitale continuïteit

Met de komst van de wet moeten accountants strenger toetsen op cyber risico's. Wanneer er geen aantoonbare cyberbeveiliging is, komen er in de jaarrekening of het jaarverslag bevindingen over tekortkomingen in de beveiliging.

1 Zien hoe het werkt?

Het MKB heeft veel redenen om mee te doen

Maar liefst 50.000 – 100.000 mkb-bedrijven hebben straks een “license to operate” nodig.

8 Certificering wordt een ‘license to operate’

Digitale veiligheid is een essentieel onderdeel van de wettelijke verplichting tot ‘Goed bestuur’. Dat betekent: het waarborgen van continuïteit, het vermijden van risico's en het behouden van vertrouwen. Het NIS2-certificaat vormt in dat licht een echte ‘license to operate’: het tastbare bewijs dat je organisatie haar digitale veiligheid aantoonbaar op orde heeft.

5 Je Cybersecurity aantoonbaar op orde telt bij bedrijfsvername

Bij een bedrijfsverkoop wordt steeds vaker gekeken naar cyberweerbaarheid. Zonder aantoonbare beveiliging daalt de waarde van een bedrijf of gaat de verkoop niet door. Certificering kan dit voorkomen.

6 Cyberverzekeringen stellen strengere eisen

Verzekeraars scherpen hun voorwaarden aan. Zonder aantoonbaar je cybersecurity op orde, zoals een NIS2 Quality Mark certificaat, kan dekking worden geweigerd of moet je eerst veel papierwerk doen of een controle ondergaan. Net als bij brandverzekeringen wordt preventie de norm.

7 Certificering via een audit levert het bewijs

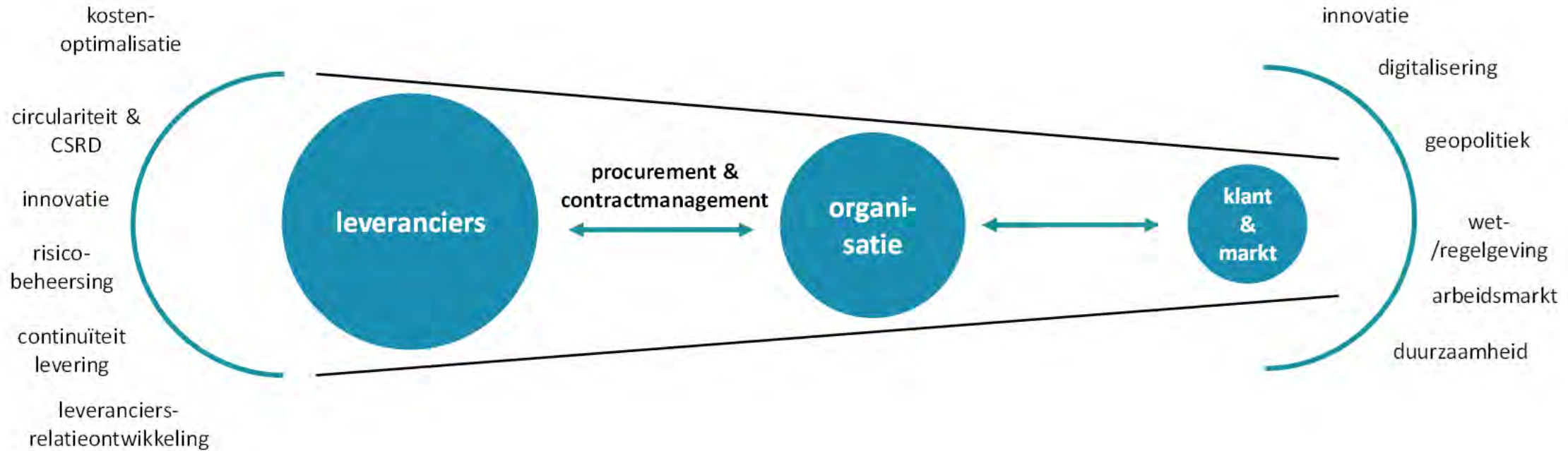
Steeds meer bedrijven en organisaties vragen dus om een adequaat bewijs van digitale veiligheid. Via een onafhankelijke audit krijg je een NIS2-certificaat en toon je aan dat cybersecurity op orde is. We doen tegenwoordig zoveel van ons werk digitaal. Dit is het logische gevolg.



Mkb-bedrijven kunnen verlies van grote klanten voorkomen

NIS2 verplicht 8.000-10.000 NIS2 bedrijven en organisaties om hun leveranciers te controleren op digitale veiligheid. Dit raakt naar schatting 50.000 – 100.000 mkb-bedrijven. Wie zijn cybersecurity niet aantoonbaar op orde heeft, loopt het risico waardevolle klanten te verliezen. Dat risico is te groot om te negeren.

Impact procurement



**leveranciers beïnvloeden 60-85%
van het succes van jouw organisatie**

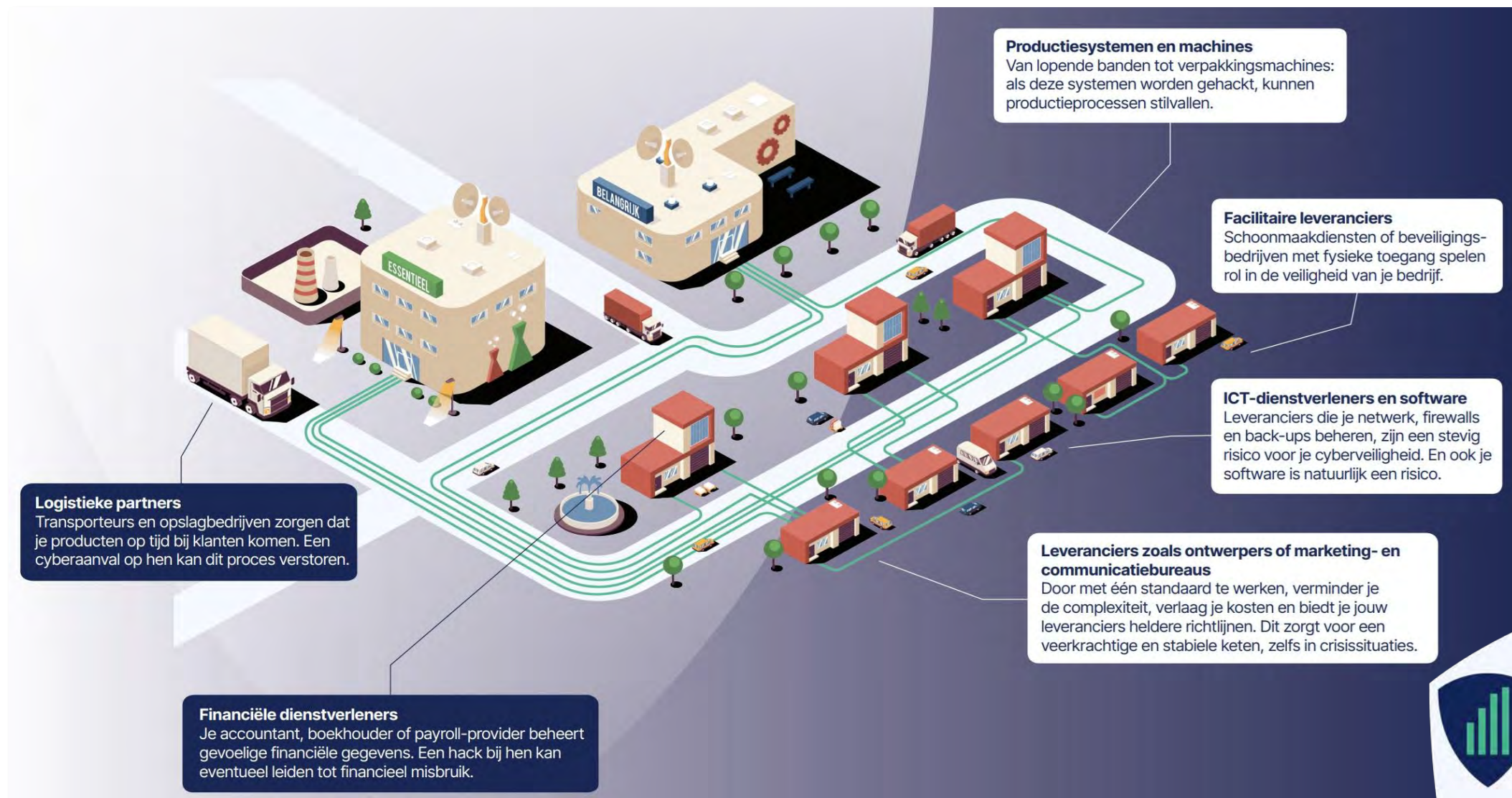


Inkoopvoorwaarden met cybersecurity verplichting wordt de standaard.

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'.



Beveiliging toeleveringsketen verplicht



Risico's bij leveranciers regelen

- **Financiële belangen** (financieel / fiscaal / Accountancy)
- **Juridische belangen** (juridisch advies)
- **Veiligheidsbelangen** (bewaking, software, opslag, etc...)
- **Operationele belangen** (IT, machines, transport, grondstoffen, etc...)
- **Reputatiebelangen** (consultancy, marketing, onderzoek, etc...)
- **Personeelsbelangen** (arbo, training, werving en selectie, etc...)
- **Strategische belangen** (consultancy, data, innovatie, etc...)
- **Klantbelangen** (CRM, Cloud, web, marketing, etc...)
- **Innovatiebelangen** (onderzoek, data, IT, octrooien, etc...)
- **Omgevingsbelangen** (afval, chemie, milieu, etc...)
- **Leveranciers- en partnerbelangen** (DMS-systeem, juridisch advies, projectmanagement, etc..)
- **Product gerelateerde belangen** (export/import, product design, productie, etc...)
- **Gegevensbeschermingsbelangen** (IT-systemen, cloud opslag, notaris, etc...)

<https://samendigitaalveilig.nl/te-beschermen-belangen/>

Wat zegt de wet?

NIS2- Artikel 21.2d: "de beveiliging van de toeleveringsketen, inclusief beveiliging gerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar directe leveranciers of dienstverleners."

NIS2 organisaties zijn aansprakelijk:

- ☐ **Risico inventarisatie maken**
- ☐ **Contractuele afspraken maken met je leveranciers**
- ☐ **Toetsen op compliance**
- ☐ **Blijvende zorgplicht**



Risiconiveau-inventarisatie

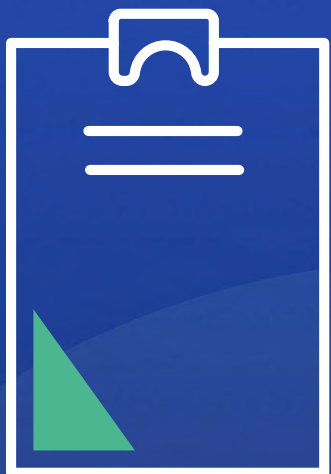
Voorbeeldvragen

- ✓ Gebruik je digitale systemen van deze leverancier binnen de bedrijfsvoering?
- ✓ Zijn er fysieke afhankelijkheden waardoor het primaire proces een risico loopt?
- ✓ Is er regelmatig e-mailverkeer met de leverancier door één of meerdere van je medewerkers en één of meerdere medewerkers van de leverancier?
- ✓ Gebruik je OT-systemen, apparatuur van deze leverancier binnen de bedrijfsvoering?
- ✓ Hoe lang kun je zonder de producten en/of dienstverlening van deze leverancier zonder dat de bedrijfsvoering wordt verstoord?

Details

- ✓ Maak een risico-inventarisatie van al je leveranciers
- ✓ Bepaal het risiconiveau
- ✓ Leg een passende cybersecurity norm op
- ✓ Leg die norm vast in je inkoopvoorwaarden / contracten
- ✓ Ontvang het bewijs van de audit dat de leverancier eraan voldoet

IT, Inkoop en je cybersecurityspecialist werken samen voor passende maatregelen

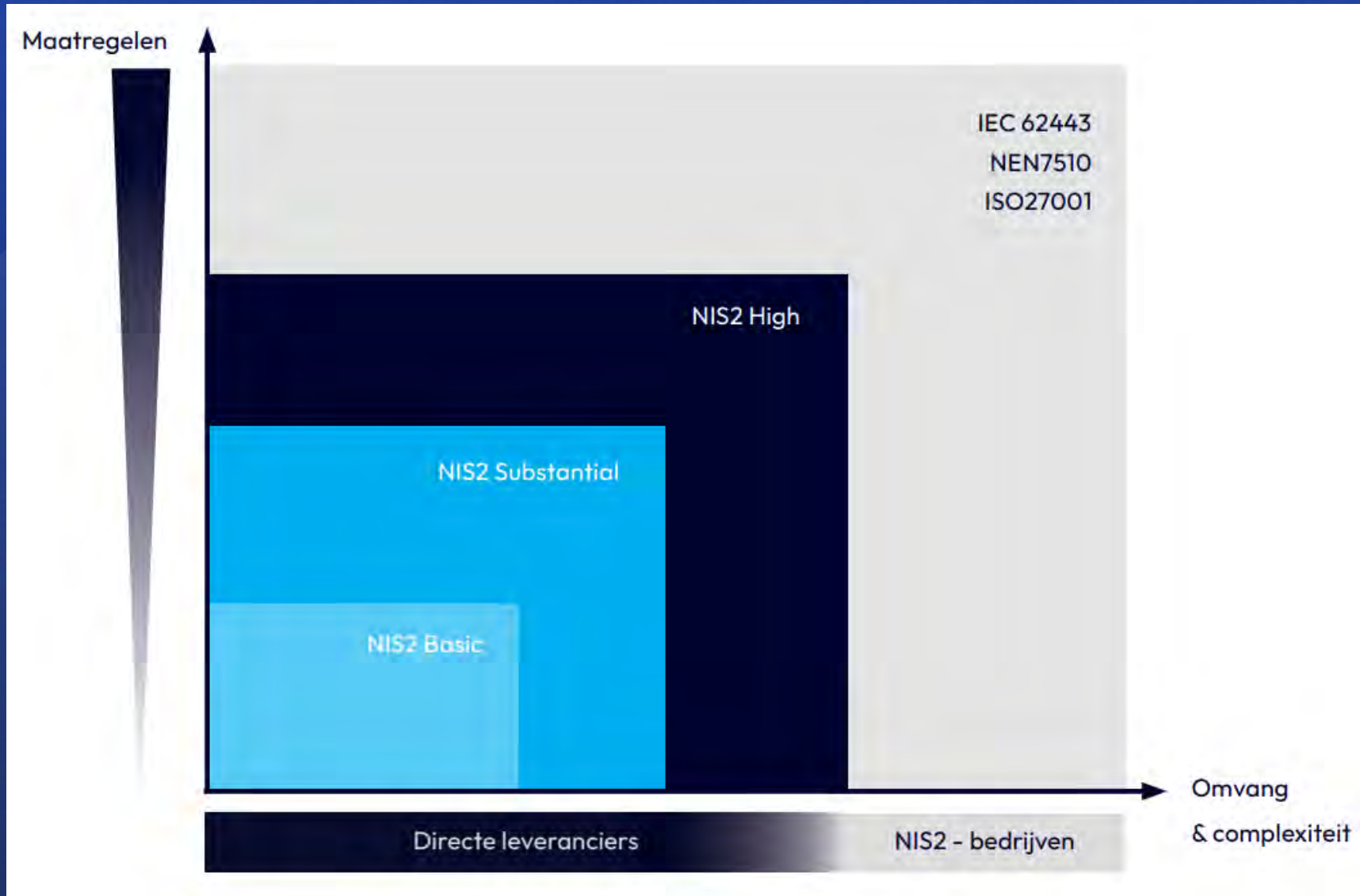


Certificering via een audit levert het bewijs

Steeds meer bedrijven en organisaties vragen dus om een adequaat bewijs van digitale veiligheid.

Met het NIS2 Supply Chain certificaat toon je (als leverancier) aan dat cybersecurity op orde is.

De norm voor de toeleveringsketen



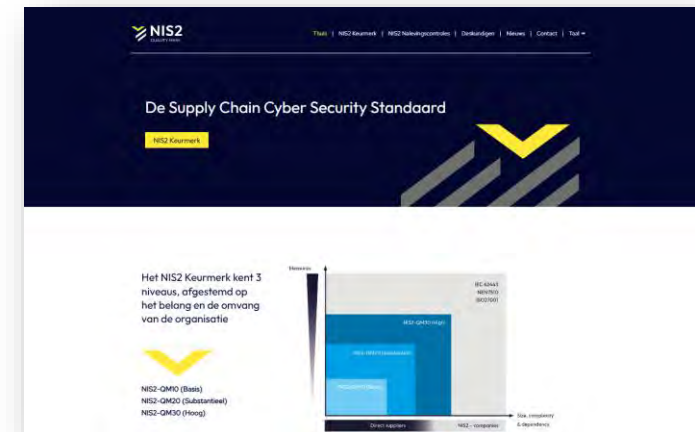
Twée initiatieven: Samen Sterk!

Samen Digitaal Veilig



- ✓ >100 branches & >90 kennis- en marktpartijen
- ✓ Praktische tools en hulpmiddelen
- ✓ Maatregelenlijsten NIS2 Quality Mark
- ✓ 1-op-1 ondersteuning & helpdesk

NIS2 SUPPLY CHAIN



- ✓ Standaard normering cybersecurity & NIS2
- ✓ Open norm: door iedereen te gebruiken
- ✓ 3 niveaus: Basic / Substantial / High
- ✓ Audit en certificering mogelijk

Kies een haalbare norm voor je leveranciers



“Cybersecurity is niet af te spreken zonder norm.”

“Normen kosten tijd en geld. Kies verstandig”

“Leveranciers moeten op tijd beginnen.”

Wat kan je nu doen?

- Ga naar de website: <https://nevi.nl/nis2>
- Ga naar de website: <https://samendigitaalveilig.nl/inkoop/>
- Hier vind je informatie en praktische hulpmiddelen
- Breng je leveranciers en de risico's in kaart
- Gebruik hiervoor Samen Digitaal Veilig
- Informeer je leveranciers tijdig!
- Leg passende maatregelen op (via NIS2 SC norm)
- Stel aanvullende eisen via je inkoop voorwaarden



NIS2 Quality Mark certificering

Ingebouwd in Samen Digitaal Veilig