EKCO

The people who power your possible ...

EKCO

Webinar
NIS2 als kans

Henk Bijsterbosch & Jacco Wildeman

6 mei 2025

1000+
Wereldwijde IT professionals

110+
Nederlandse IT professionals

250+
Security specialisten

42 jaar
IT, beheer & beveiliging

17 jaar
Cloud

4,5 / 5
Kwaliteitswaardering

Jacco Wildeman
Security Solution Consultant
linkedin.com/in/jacco-wildeman

Microsoft Solutions Partner
Modern Work
Specialist
Modern Work

Microsoft Solutions Partner
Infrastructure Azure
Specialist
Azure Virtual Desktop

Microsoft Solutions Partner
Security
Specialist
Cloud Security

Microsoft Solutions Partner
Security
Specialist
Identity & Access Management

Microsoft Solutions Partner
Security
Specialist
Information Protection & Governance

Microsoft Solutions Partner
Security
Specialist
Threat Protection

DELL Technologies GOLD PARTNER

FORTINET

vmware Principal Partner Cloud Provider

Extreme networks

veeam Cloud & Service Provider Platinum

Agenda

1. NIS2: wat is het ook alweer?
2. Ketenzorgplicht: belangrijke te nemen stappen
3. NIS2 Quality Mark toegelicht
4. Zo werkt het auditingproces
5. Wie houdt toezicht en hoe werkt dat?
6. Aan de slag: waar/hoe begin je?

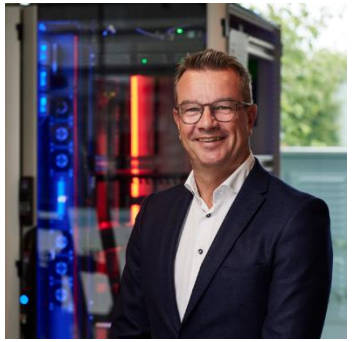
NIS2 als kans

Vraag

Hoe staat jouw organisatie ervoor met NIS2?

1. Geen idee of NIS2 op ons van toepassing is.
2. Niet plichtig, maar verwachten wel actie via leveranciers.
3. Plichtig, maar nog zoekende wat te doen.
4. Plichtig, bezig met behalen van QM.
5. Plichtig en ISO 27001-gecertificeerd.
6. Plichtig en QM30-gecertificeerd.

Even voorstellen



- Henk Bijsterbosch
- Manager kennispartners
- ✆ 06-10279705
- ✉ hb@samendigitaalveilig.nl
- Eigenaar: Fortune Consultancy

- Ervaring
  - Consultancy & Advies (oa. NIS2, Change mngt, Proces mngt)
  - Interim Management
  - Commercieel Directeur Cybersecurity, Infrastructure & Werkplek
  - Stagebegeleider & Assessor HAN

Cybersecurity NIS2 wetgeving & ketenverantwoordelijkheid

EKCO

Samen Digitaal Veilig

NIS2 in één overzicht

In Nederland zal de Cyberbeveiligingswet ingaan per Q3 2025

	# Werknemers		Jaaromzet		Balanstotaal
Grote Organisaties	=> 250	*of*	> 50 mln	+	> 43 mln
Middelgrote Organisaties	=> 50	*of*	> 10 mln	+	> 10 mln

Zeer kritieke sectoren	*Grote organisaties*	*Middelgrote organisaties*	*Kleine- en micro organisaties*
Energie	✓	✓	✗
Transport	✓	✓	✗
Bankwezen	✓	✓	✗
Infrastructuur financiele Markt	✓	✓	✗
Gezondheidszorg	✓	✓	✗
Drinkwater	✓	✓	✗
Digitale infrastructuur	✓	✓ ✓	✓ ✓
Beheerders van ICT Diensten	✓	✓	✗
Afvalwater	✓	✓	✗
Overheidsdiensten	✓	✓	✓
Lokale overheden	✓	✓	✓
Ruimtevaart	✓	✓	✗

✓ *Essentiele entiteit*
✓ Belangrijke entiteit
✗ niet van toepassing

Andere kritieke sectoren	*Grote organisaties*	*Middelgrote organisaties*	*Kleine- en micro organisaties*
Digitale aanbieders	✓	✓	✗
Post- en koeriersdiensten	✓	✓	✗
Afvalstoffenbeheer	✓	✓	✗
Levensmiddeleen	✓	✓	✗
Chemische stoffen	✓	✓	✗
Onderzoek	✓	✓	✗
Vervaardiging	✓	✓	✗

Samen Digitaal Veilig

Hoofdpunten van de Cyberbeveiligingswet

- Registratieplicht
- Meldplicht
- Zorgplicht
- Toezicht

Samen Digitaal Veilig

Zorgplicht

De 10.000 grote NIS2 organisaties moeten zichzelf volledig aantoonbaar beveiligen.

+

Verplicht de risico's analyseren en vervolgens beveiliging van de toeleveringsketen regelen.

1. Een risicoanalyse en beveiliging van Informatiesystemen;
2. Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van assets;
3. Maatregelen op het gebied van bedrijfcontinuïteit, zoals back-up beheer en noodvoorzieningenplannen;
4. Incidentenbehandeling;
5. Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging;
6. Beveiligen bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, incl. de respons op en bekendmaking van kwetsbaarheden
7. Beveiliging van de toeleveringsketen
8. Beleid en procedures over het gebruik van cryptografie en encryptie;
9. Het gebruik van Multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen
10. Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen

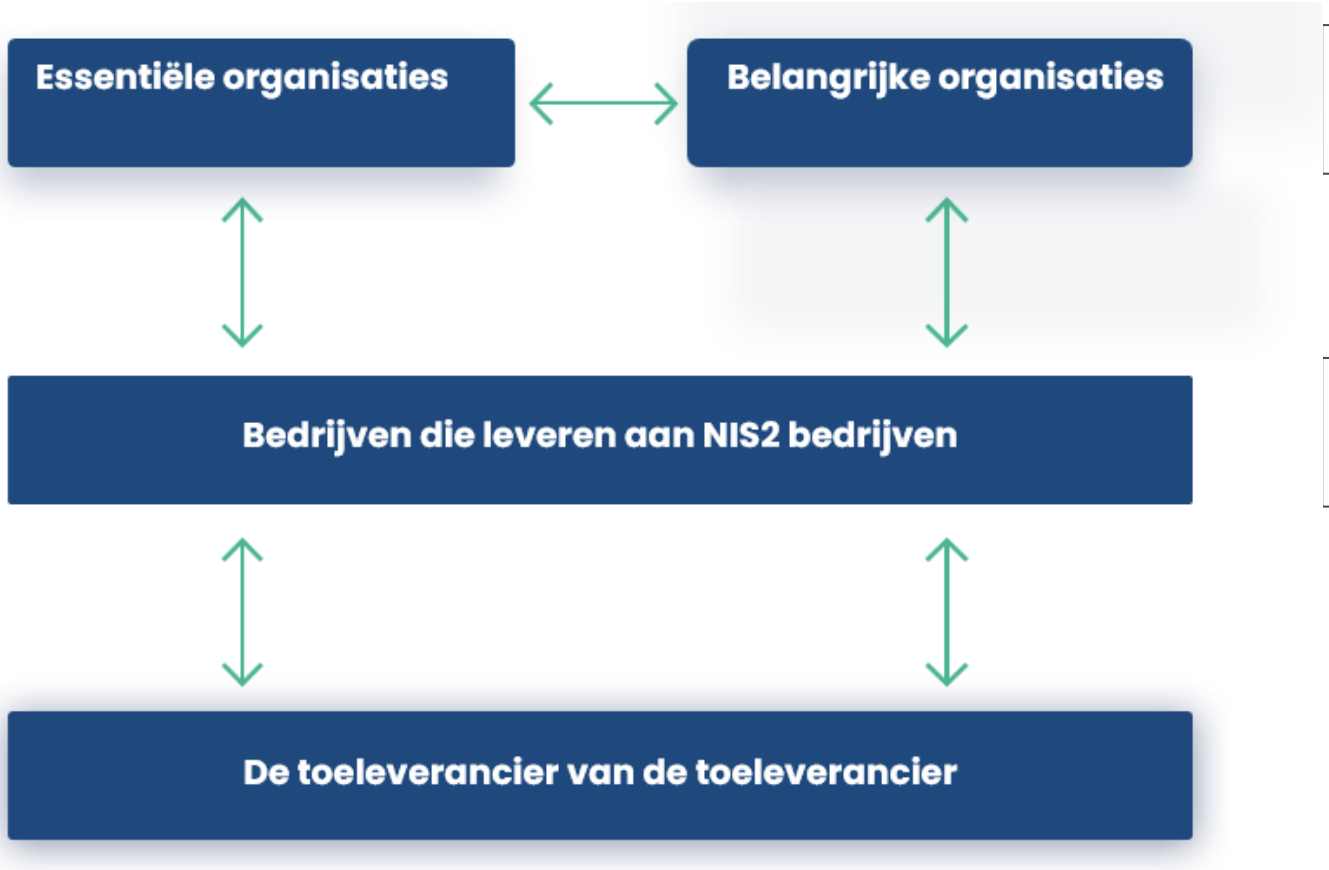
Samen Digitaal Veilig

Samen Digitaal Veilig

NIS2 en alle bedrijven in de keten

Uitdaging

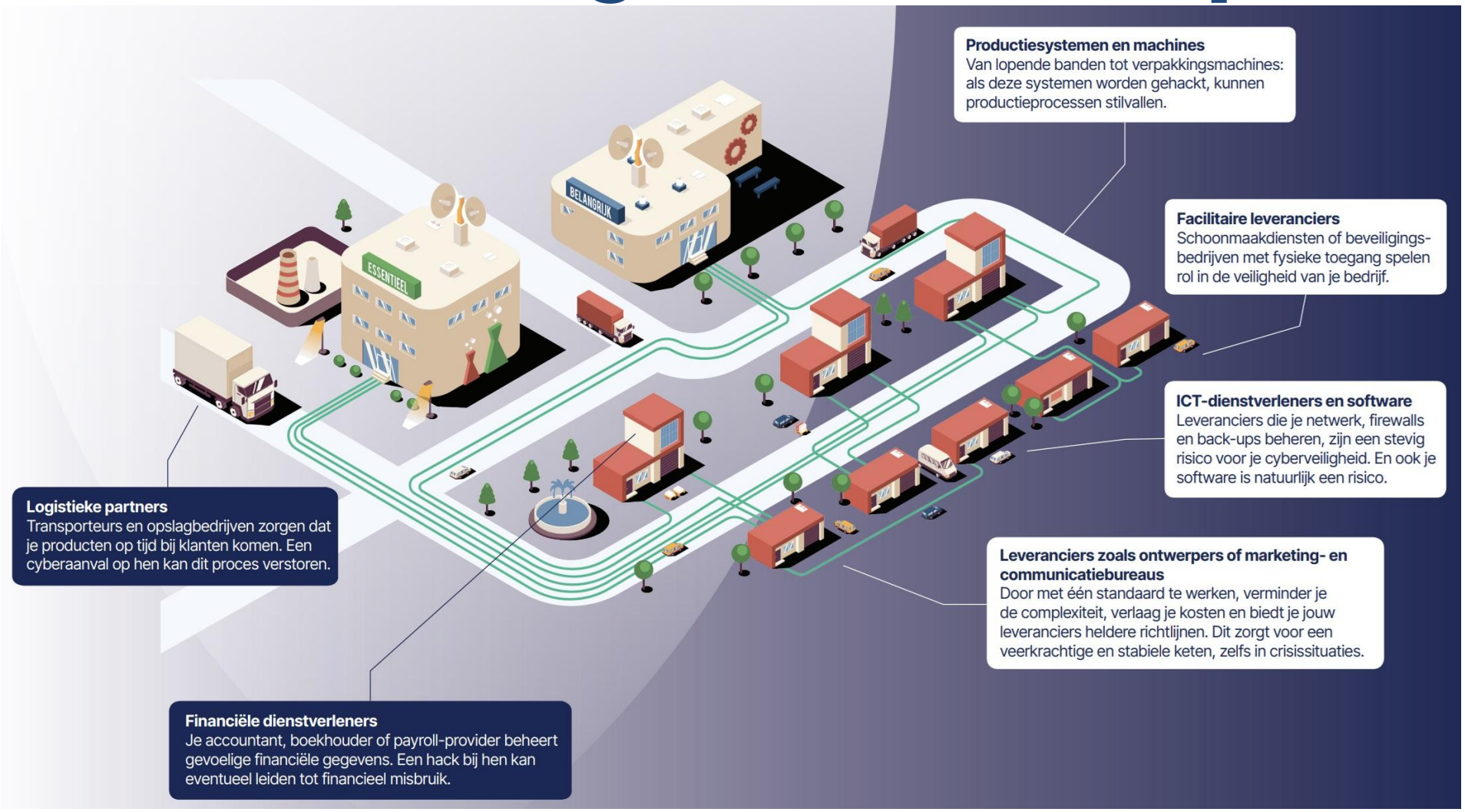
Ruim 50.000 leveranciers van NIS2 bedrijven moeten bewijzen dat ze veilig digitaal werken



10.000 NIS2 bedrijven

50.000 + leveranciers

NIS2 wetgeving: de beveiliging van de toeleveringsketen is verplicht



Risico bij alle bedrijven https://samendigitaalveilig.nl/te-beschermen-belangen/

Samen Digitaal Veilig

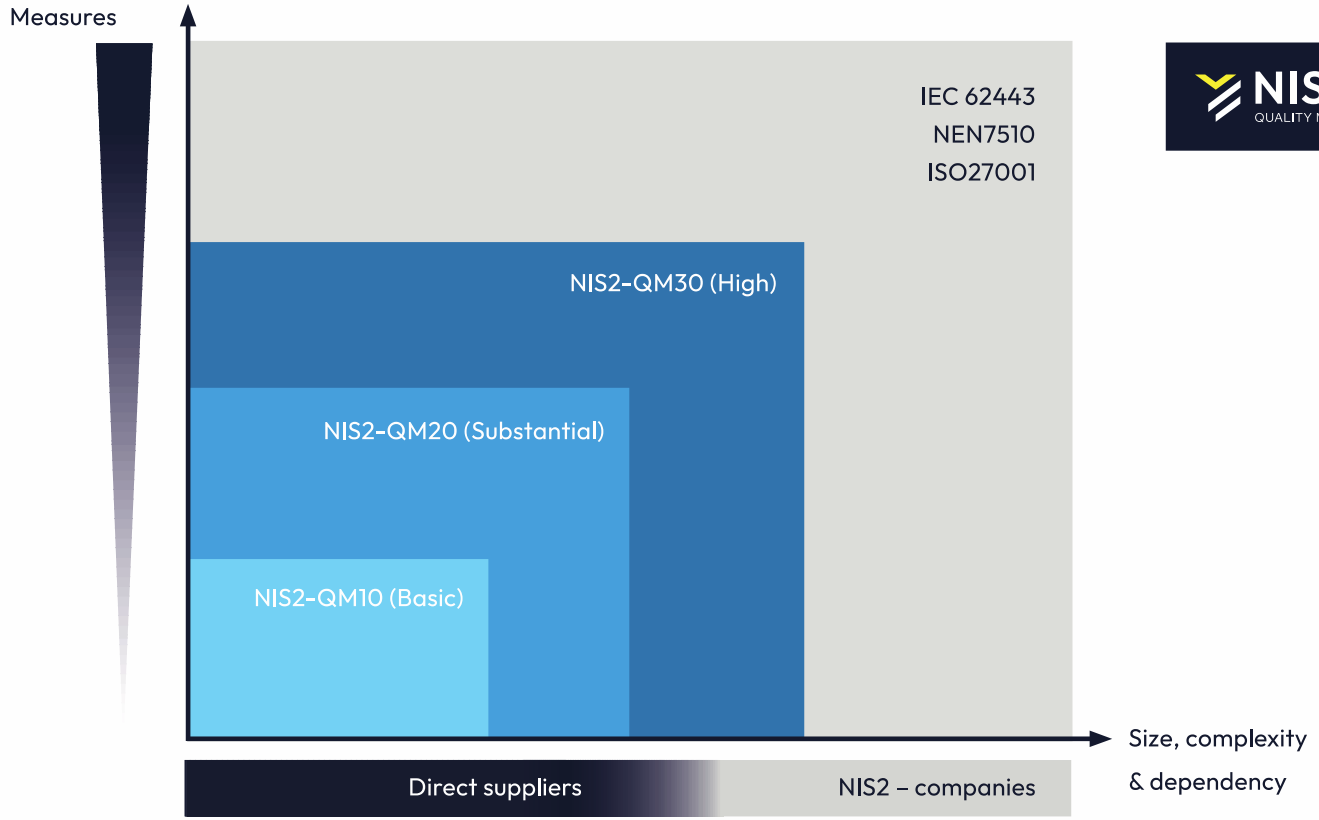
NIS2 Quality Mark

De cyberveiligheidsnorm voor de toeleveringsketen

NIS2
QUALITY MARK 6 mei 2025

Bij risico passende niveaus

- NIS2 Quality Mark kent 3 niveaus, afgestemd op het belang en de omvang van de organisatie



- NIS2-QM-10 (Basic)
- NIS2-QM-20 (Substantial)
- NIS2-QM-30 (High)

GAP NIS2 met ISO27001

Veel bedrijven denken dat ze compliant zijn zodra ze bijv. ISO27001 hebben behaald. Maar dat is een misvatting.
Er zijn belangrijke verschillen geïdentificeerd, zoals:

- ✓ 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 ISO27001.

Samen Digitaal Veilig

NIS2 QUALITY MARK

Het certificeringsproces in vijf stappen

1. Pre-registratie

De eerste stap richting certificering

2. Audit voorbereiding

.

3. Pre-audit webinar

Bereid je optimaal voor

4. Certificering

Een onafhankelijke audit bepaalt of jouw organisatie voldoet aan de NIS2 QM-standaarden. Kies een Auditor

5. Officieel NIS2-QM-certificaat

Wat biedt pre-registratie?

- Een pre-registratiebewijs als teken van je inzet voor NIS2 compliance.
- Toestemming om het NIS2 QM-logo en de QR-code te gebruiken.
- De mogelijkheid om een audit aan te vragen bij een erkende auditor.

Een audit kan een uitdaging zijn, maar met de juiste voorbereiding vergroot je de kans op een succesvolle certificering. In ons pre-audit webinar begeleiden we je door het volledige proces en geven we je praktische handvatten om optimaal voorbereid te zijn.

Toezicht

Er komen 7 toezichthouders

- **RDI** (Rijksinspectie Digitale Infrastructuur)
- **ILT** (Inspectie Leefomgeving en Transport)
- **IGJ** (Inspectie Gezondheidszorg & jeugd)
- **AP** (Autoriteit Persoonsgegevens)
- **ANVS** (Autoriteit Veiligheid en Stralingsbescherming)
- **DNB** (De Nederlandse Bank)
- **AFM** (Autoriteit Financiële Markten)

Samen Digitaal Veilig

Hoe werkt Toezicht?

- Stimuleren van actief werken aan digitale weerbaarheid
  - Initieel: Controlerend en stimulerend
- Verbinding zoeken met de sectoren
- Pro-actief (Essentiele sectoren) & Reactief (Belangrijke sectoren)
- Probleem- en risicogericht
- Toezicht wordt gezien als maatwerk (geen 'one size fits all')
- In uiterste geval: dwangmiddelen (o.a. boetes)

Samen Digitaal Veilig

Aan de slag .....

https://www.ek.co/nl/nis2-kennisbank/

Plan van Aanpak

- **IT** afdeling is de traditionele plek waar cybersecurity wordt geregeld
- **HR** voor opleidingen
- **Legal** voor de contracten
- **Inkoop** voor de leveringsketen

- **Creëer een multidisciplinair team**
- **Beleid voor procedures en borging**
- **Zorg voor rapportages**

Samen Digitaal Veilig

De 100 verzamelde brancheorganisaties + deelnemende kennis- en marktpartijen wijzen bedrijven de weg

- Voldoen aan de wet
- Alles in begrijpelijke taal
- Met ondersteuning van Samen Digitaal Veilig & EKCO is het goed realiseerbaar voor ieder bedrijf

www.samendigitaalveilig.nl

Aan de slag

Prijs vanaf
€480 / per jaar

Haal je NIS2-certificering

- Speciaal voor mkb-bedrijven (leveranciers)
- Maatregelenlijst en alle cybersecuritymaatregelen (compleet)
- Training voor medewerkers via 28 video's en vragenlijst
- Complete leveranciersrisicoanalyse van alle externe partijen
- Alle uitleg documenten kant en klaar bruikbaar
- Invul webinars voor de maatregelen en leveranciersrisico's
- Persoonlijk 1-op-1 opstartgesprek

Haal je NIS2 Quality Mark

Meer informatie →

Prijs vanaf
€2.750 / per jaar

NIS2 Corporate Supply Chain pakket

- Speciaal voor NIS2-entiteiten
- Maatregelenlijst en alle cybersecuritymaatregelen (compleet)
- Training voor medewerkers via 28 video's en vragenlijst
- Complete leveranciersrisicoanalyse van alle externe partijen
- Alle uitleg documenten kant en klaar bruikbaar
- Invul webinars voor de maatregelen en leveranciersrisico's
- Persoonlijk 1-op-1 opstartgesprek
- ISO GAP NIS2 inbegrepen
- Managementdashboard

Beveiig je Supply Chain

Meer informatie →

Behaal je NIS2-certificering

Bedrijven die lid zijn van brancheorganisaties of samenwerken met een partner krijgen 50% korting. De onderstaande prijzen zijn per jaar.

Bedrijfsomvang	Standaardprijs	Prijs met 50% korting	
1 - 3 medewerkers	€ 960	€ 480	Bestel nu
4 - 7 medewerkers	€ 1.614	€ 807	Bestel nu
8 - 25 medewerkers	€ 2.400	€ 1.200	Bestel nu
26 - 100 medewerkers	€ 3.900	€ 1.950	Bestel nu
101 - 250 medewerkers	€ 6.780	€ 3.390	Bestel nu
> 250 medewerkers	Prijs op aanvraag	Prijs op aanvraag	Aanvragen

Samen Digitaal Veilig

Account aanmaken

NL

Vul onderstaande gegevens in zodat jij kunt starten met het digitaal veiliger maken van jouw organisatie.

Organisatie

Kortingscode

* Kortingscodes worden verstrekt door onze partners. Kijk hier voor onze partnerlijst. Ben je geen lid van een van onze partners, gebruik dan de tijdelijke kortingscode Tijdelijk10 om 10% korting te krijgen

Voornaam

Achternaam

E-mailadres

Ik ben een mens

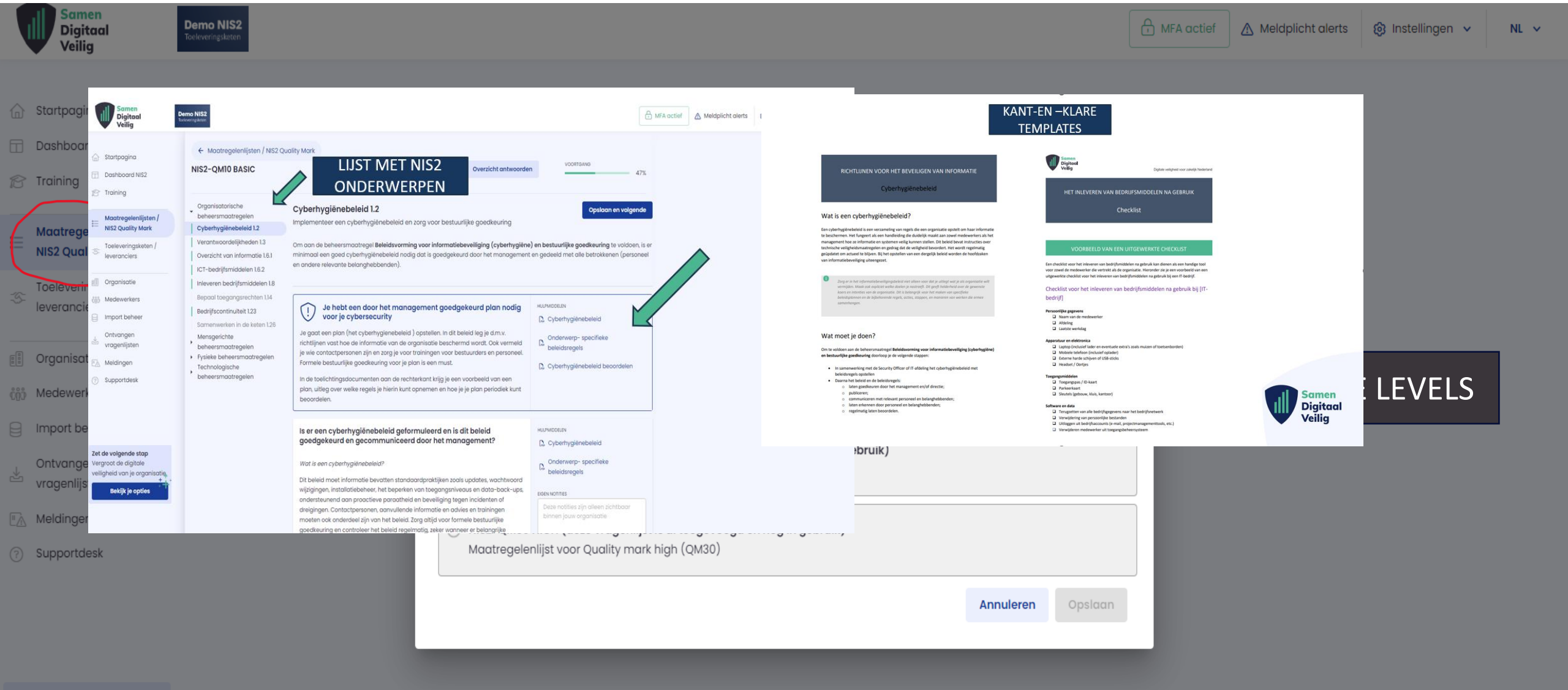
hCaptcha
Privacy - Voorwaarden

Ik ga akkoord met de algemene voorwaarden en privacy statement.

Ik heb al een account

Aanmelden

Samen Digitaal Veilig


Samen Digitaal Veilig
Demo NIS2
Toeleveringsketen
MFA actief
Meldplicht alerts
Instellingen
NL
Startpagina
Dashboard NIS2
Training
Maatregelenlijsten / NIS2 Quality Mark
Toeleveringsketen / leveranciers
Organisatie
Medewerkers
Import beheer
Ontvangen vragenlijsten
Meldingen
Supportdesk
Maatregelenlijsten / NIS2 Quality Mark
NIS2-QM10 BASIC
LIJST MET NIS2 ONDERWERPEN
Overzicht antwoorden
VOORTGANG
47%
Organisatorische beheersmaatregelen
Cyberhygiënebeleid 1.2
Verantwoordelijkheden 1.3
Overzicht van informatie 1.6.1
ICT-bedrijfsmiddelen 1.6.2
Inleveren bedrijfsmiddelen 1.8
Bepaal toegangsrechten 1.14
Bedrijfscontinuïteit 1.23
Samenwerken in de keten 1.26
Mensgerichte beheersmaatregelen
Fysieke beheersmaatregelen
Technologische beheersmaatregelen
Cyberhygiënebeleid 1.2
Implementeer een cyberhygiënebeleid en zorg voor bestuurlijke goedkeuring
Opslaan en volgende
Om aan de beheersmaatregel Beleidsvorming voor informatiebeveiliging (cyberhygiëne) en bestuurlijke goedkeuring te voldoen, is er minimaal een goed cyberhygiënebeleid nodig dat is goedgekeurd door het management en gedeeld met alle betrokkenen (personeel en andere relevante belanghebbenden).
Je hebt een door het management goedgekeurd plan nodig voor je cybersecurity
Je gaat een plan (het cyberhygienebeleid) opstellen. In dit beleid leg je d.m.v. richtlijnen vast hoe de informatie van de organisatie beschermd wordt. Ook vermeld je wie contactpersonen zijn en zorg je voor trainingen voor bestuurders en personeel. Formele bestuurlijke goedkeuring voor je plan is een must.
In de toelichtingsdocumenten aan de rechterkant krijg je een voorbeeld van een plan, uitleg over welke regels je hierin kunt opnemen en hoe je je plan periodiek kunt beoordelen.
HULPMIDDELEN
Cyberhygiënebeleid
Onderwerp- specifieke beleidsregels
Cyberhygiënebeleid beoordelen
Is er een cyberhygiënebeleid geformuleerd en is dit beleid goedgekeurd en gecommuniceerd door het management?
Wat is een cyberhygiënebeleid?
Dit beleid moet informatie bevatten standaardpraktijken zoals updates, wachtwoord wijzigingen, installatiebeheer, het beperken van toegangsniveaus en data-back-ups, ondersteunend aan proactieve paraatheid en beveiliging tegen incidenten of dreigingen. Contactpersonen, aanvullende informatie en advies en trainingen moeten ook onderdeel zijn van het beleid. Zorg altijd voor formele bestuurlijke goedkeuring en controleer het beleid regelmatig, zeker wanneer er belangrijke
EIGEN NOTITIES
Deze notities zijn alleen zichtbaar binnen jouw organisatie
Zet de volgende stap
Vergroot de digitale veiligheid van je organisatie
Bekijk je opties
KANT-EN –KLARE TEMPLATES
RICHTLIJNEN VOOR HET BEVEILIGEN VAN INFORMATIE
Cyberhygiënebeleid
Wat is een cyberhygiënebeleid?
Wat moet je doen?
HET INLEVEREN VAN BEDRIJFSMIDDELEN NA GEBRUIK
Checklist
VOORBEELD VAN EEN UITGEWERKTE CHECKLIST
Checklist voor het inleveren van bedrijfsmiddelen na gebruik bij [IT-bedrijf]
Maatregelenlijst voor Quality mark high (QM30)
Annuleren
Opslaan
LEVELS

Samen Digitaal Veilig

Demo NIS2
Toeleveringsketen

MFA actief | Instellingen | NL

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

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

8
Toeleveringsketen / leveranciers

+ Toevoegen | Risicoprofiel instellen | Verwijderen

Zoeken

Leverancier	Risico-inventarisatie	Risicoprofiel	Certificaat	Notitie	Status	Bewerk
A-B Fast Routeplanning software	RI gereed (Advies: Hoog)	Hoog			Dringend actie	
ASPA International	RI gereed (Advies: Hoog)	Hoog			Bezig	
ABC Truck chemicals cleaning	RI gereed (Advies: Hoog)	Substantieel			Dringend actie	
Accountantcy Lexicon	RI gereed (Advies: Substantieel)	Basis			Gereed	
MF bv	RI gereed (Advies: Hoog)	Basis			Bezig	
Testgroep	RI bezig	Geen			Niet gestart	
GEEN RISICO	RI bezig	Geen			Gereed	
Tech1	RI bezig	Niet ingesteld			Bezig	

6 mei 2025

© 2025 | Samen Digitaal Veilig | Disclaimer | Privacy | Algemene voorwaarden

Samenvattend

1. Maak van NIS2 een **prioriteit**
   (en raak je (grote) klanten niet kwijt)

2. Gezamenlijke inspanning; zet een multidisciplinair team op

3. Maak je leveranciers bewust van hun verantwoordelijkheden en ondersteun bij het implementeren van de juiste maatregelen

4. Haal je eigen NIS2 certificering (NIS2 Quality Mark)

5. **Samen Digitaal Veilig & Ekco** ondersteunen met **platform** en praktische hulpmiddelen

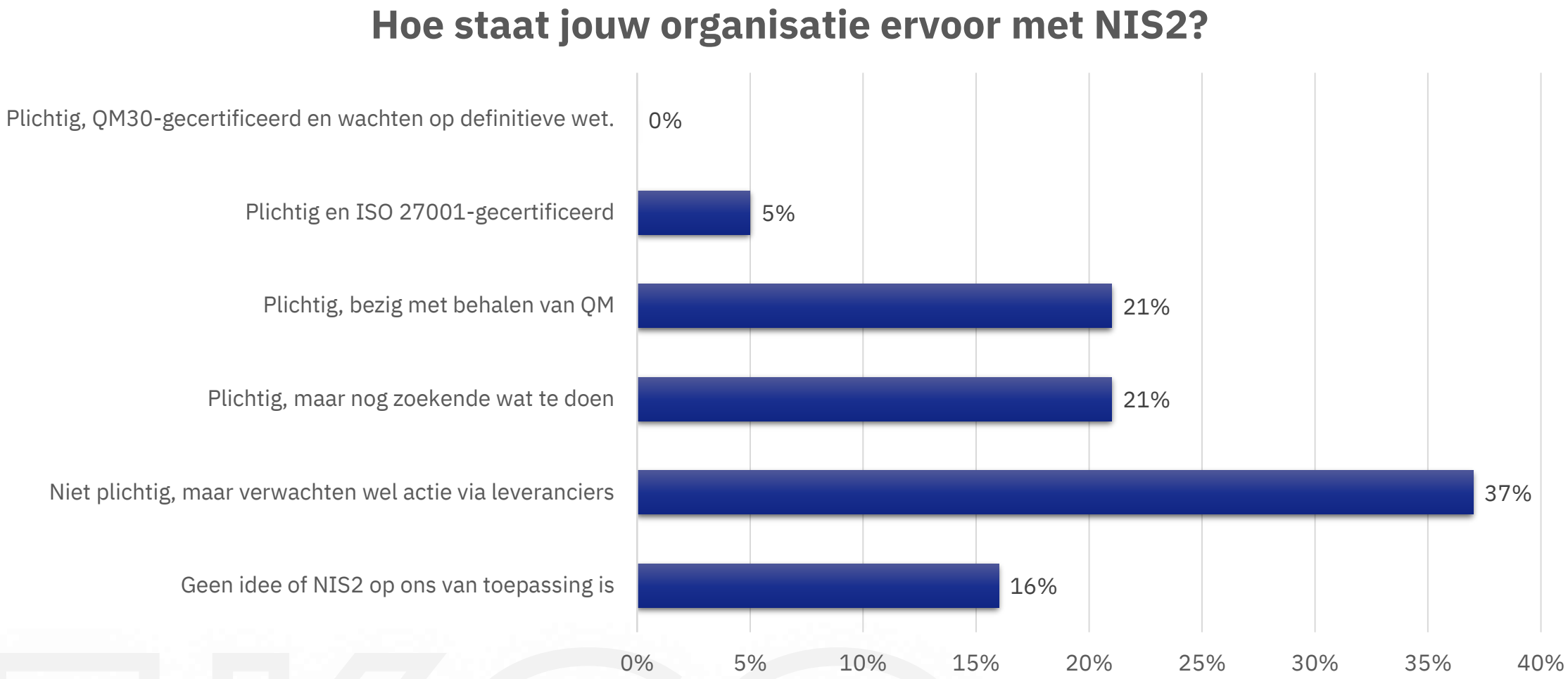
Samen Digitaal Veilig

Welke stappen je moet zetten

NIS2 als kans

Poll

Resultaat



Zelf evaluatie

- Geen idee of NIS2 op ons van toepassing is.

NIS2 als kans

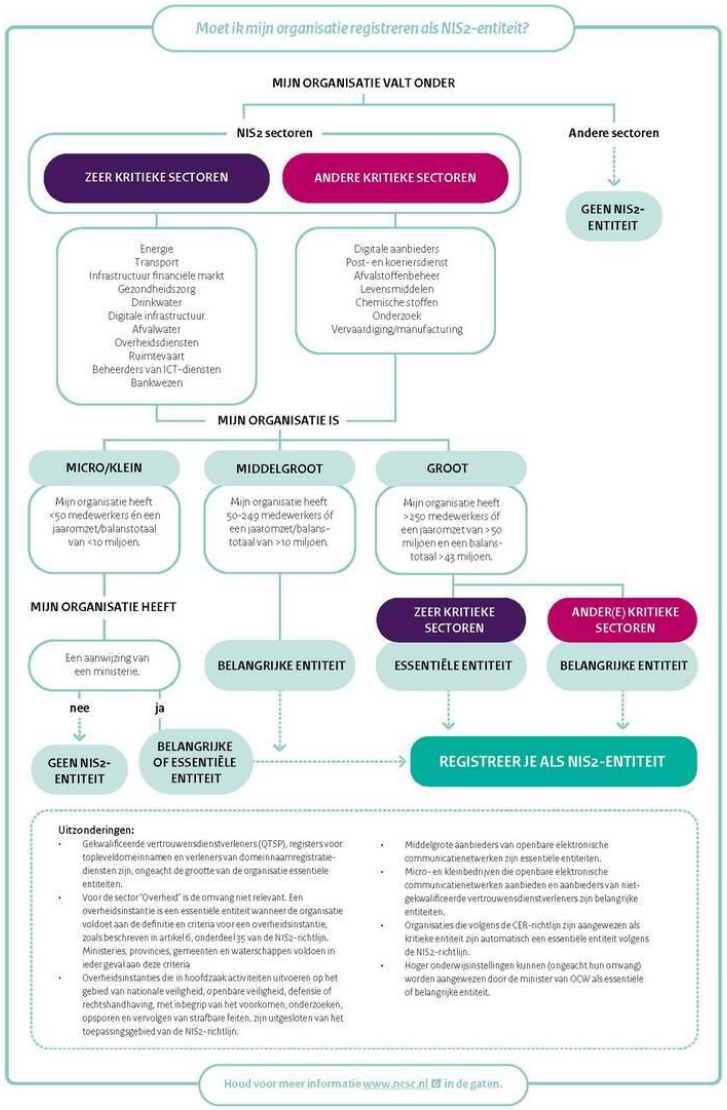
Valt jouw organisatie onder de NIS2?

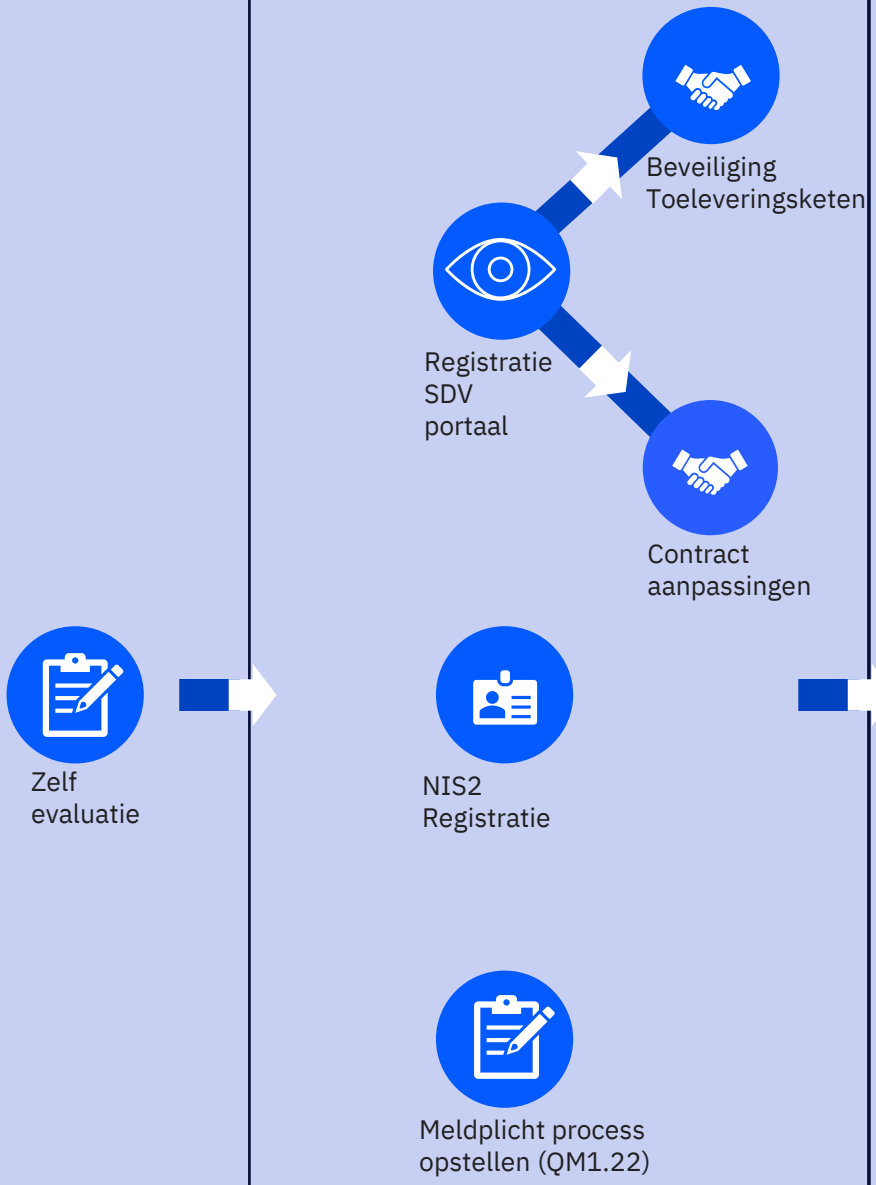
Een belangrijk verschil met de eerste NIS-richtlijn is, dat organisaties automatisch onder de NIS2-richtlijn vallen als zij actief zijn in bepaalde sectoren en volgens bepaalde criteria als **'essentiële'** of **'belangrijke'** entiteit worden aangemerkt. Automatisch betekent dit dat de verplichtingen van de NIS2-richtlijn voor deze organisaties direct van toepassing worden zodra de nationale wetgeving in werking treedt.

Zelfevaluatie NIS2

In nauwe afstemming met de betrokken ministeries en toezichthouders heeft de Rijksinspectie Digitale Infrastructuur (RDI) een vragenlijst ontwikkeld waarmee organisaties zelf kunnen evalueren of zij onder de NIS2-richtlijn vallen en of zij als essentieel of belangrijk worden aangemerkt.

https://regelhulpenvoorbedrijven.nl/NIS-2-NL/





- Geen idee of NIS2 op ons van toepassing is.

- Plichtig, maar nog zoekende wat te doen.
- Plichtig, bezig met behalen van QM.
- Plichtig en ISO 27001-gecertificeerd.

NIS2 als kans

Registratieplicht

In Nederland vindt de registratie plaats bij het Nationaal Cyber Security Centrum (NCSC)

De NIS2-richtlijn heeft als doel de digitale weerbaarheid van essentiële en belangrijke diensten en organisaties in Europa te verbeteren. Deze organisaties zijn wettelijk verplicht om gegevens aan te leveren voor het entiteitenregister, waarmee de EU inzicht krijgt in de digitale weerbaarheid.

De registratieplicht geldt vanaf de inwerkingtreding van de wet.

1 Checklist inloggen

Via Single Sign On Rijk

Aangesloten Rijksoverheidsorganisaties kunnen eenvoudig en veilig inloggen via Single Sign On Rijk.

1. Ga naar mijn.ncsc.nl
2. Klik op Inloggen achter Single Sign On Rijk (SSOnRIJK) en doorloop de stappen

Via eHerkenning

Overige organisaties kunnen veilig inloggen via eHerkenning. Om in te loggen heb je betrouwbaarheidsniveau EH2+ nodig. Let op: zorg dat het eHerkenningsmiddel gekoppeld is aan het juiste KVK-nummer.

1. Om namens jouw organisatie de registratie te voltooien moet je gemachtigd worden via eHerkenning. De persoon die binnen jouw organisatie eHerkenning beheert, kan dit voor jou in gang zetten. Als jouw organisatie nog geen eHerkenning heeft, moet dit eerst worden aangevraagd. Kijk voor meer informatie over eHerkenning op www.eherkenning.nl
2. Ga naar mijn.ncsc.nl
3. Klik op Inloggen achter eHerkenning en doorloop de stappen
4. Klik op 'NIS2-registratie starten'

2 Checklist organisatiegegevens

In de NIS2-registratie wordt een aantal verplichte gegevens uitgevraagd. Enerzijds om te bepalen of de organisatie NIS2-plichtig is, en anderzijds om de benodigde gegevens van de NIS2-entiteiten op te nemen in het register.

- ☐ KVK-nummer. Zorg dat het eHerkenningsmiddel gekoppeld is aan het juiste KVK-nummer
- ☐ Bezoekadres. Zorg dat deze up-to-date is in het handelsregister van de KVK
- ☐ Correspondentieadres. Zorg dat deze up-to-date is in het handelsregister van de KVK
- ☐ Sector(en) waarin de organisatie actief is.
- ☐ Type NIS2-entiteit: belangrijk of essentieel. Bekijk deze flowchart of doe de self-assessmenttool van de RDI
- ☐ Type aanwijzing. Enkel in het geval van een aanwijzing van een departement of toezichthouder
- ☐ EU-lidsta(a)t(en) waarin de organisatie diensten/producten levert
- ☐ Gegevens contactpersoon organisatie (naam, telefoonnummer, e-mailadres en functietitel)
- ☐ *aantal FTE (<50 / 50 – 249 / >250)
- ☐ *Jaaromzet voorgaand kalenderjaar (<10 miljoen euro / 10 – 50 miljoen euro / >50 miljoen euro)
- ☐ *Balanstotaal voorgaand kalenderjaar (<10 miljoen euro / 10 – 43 miljoen euro / >43 miljoen euro)

** Deze punten zijn optioneel om een indicatie te geven of de organisatie een (belangrijke of essentiële) NIS2-entiteit is.*

3 Checklist netwerkgegevens

NIS2-entiteiten zijn verplicht alle netwerkgegevens op te geven. Deze assets worden gebruikt voor monitoring en ondersteuning. Je kunt de registratie afronden door minimaal 1 asset op te geven. Nadat je de registratie hebt voldaan, kun je de lijst van netwerkgegevens (in bulk) aanvullen door in te loggen op mijn.ncsc.nl.

- ☐ Minimaal 1 type asset, keuze uit:
  - (Publiek) IP-adres of -reeks
  - Domeinna(a)m(en)
  - AS-nummer (ASN)

4 Alles compleet?

Ga naar mijn.ncsc.nl en voltooi de NIS2-registratie in vijf stappen.

Kijk voor een overzicht van veelgestelde vragen en contact met het NCSC op www.ncsc.nl/contact.

https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/oktober/08/checklist-registreren/Checklist+NIS2+registratie+V2.pdf

NIS2 als kans

Meldplicht

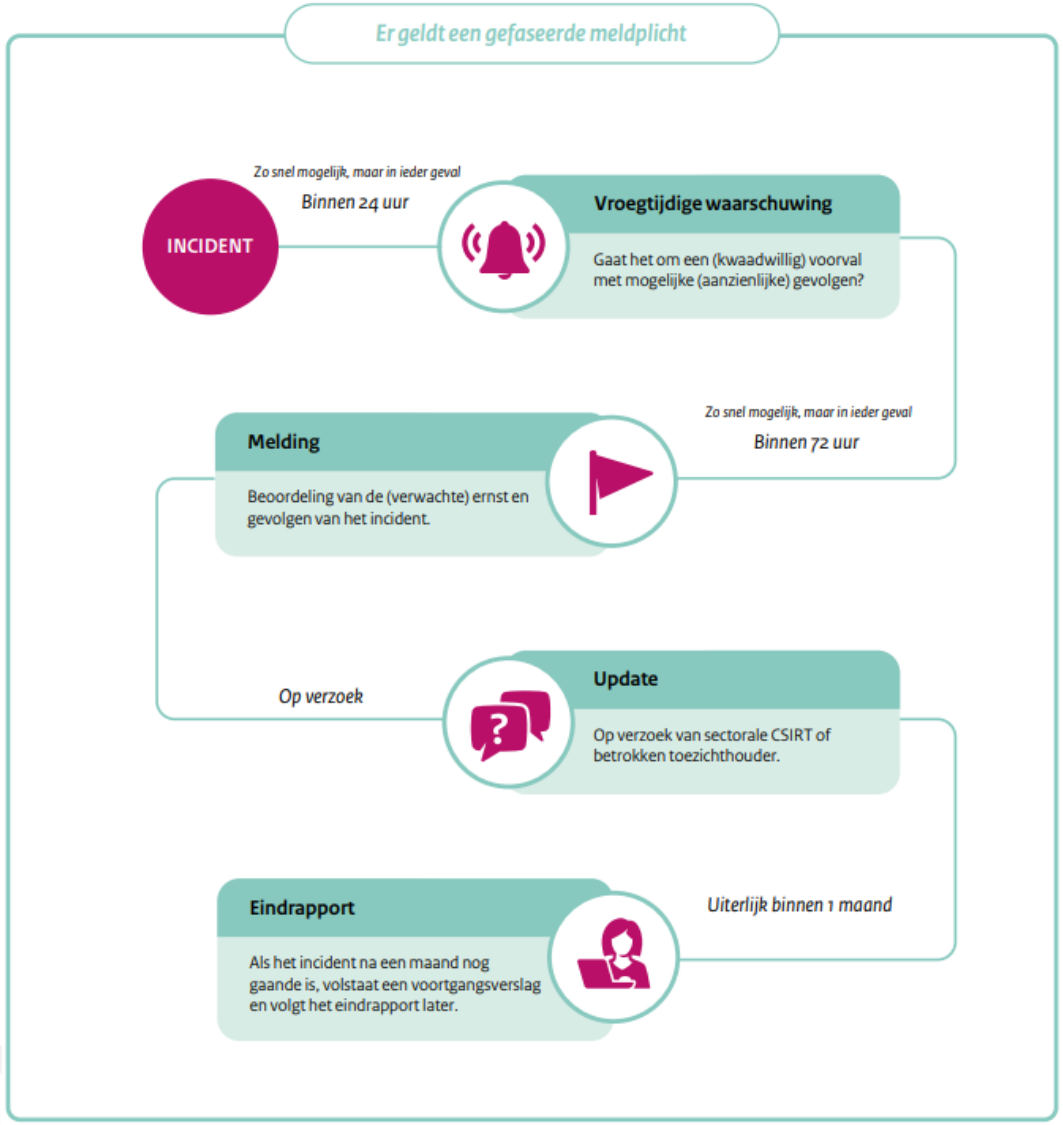
Wat voor type incidenten moet ik melden?

Significante incidenten dienen gemeld te worden bij het CSIRT en de toezichthouder. Dit zijn incidenten die de verlening van diensten van de organisatie aanzienlijk (kunnen) verstoren.

Meldingen via het NCSC meldportaal: https://www.ncsc.nl/contact/contactformulieren/incident-melden

Significante incidenten

- Als het incident een ernstige operationele verstoring van de diensten veroorzaakt of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken.
- Als het incident andere entiteiten heeft getroffen, of kan treffen door aanzienlijke materiele of immateriële schade te veroorzaken.



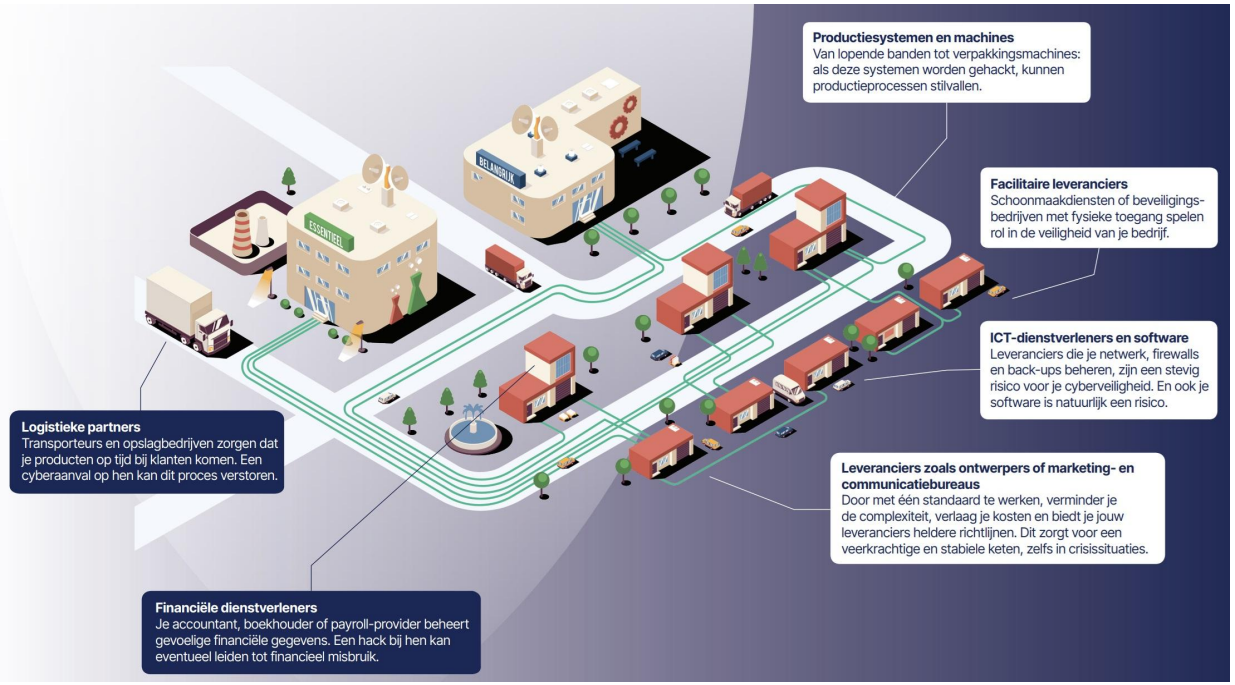
De vorm voor de meldplicht wordt pas definitief als de wet er is in Q3.

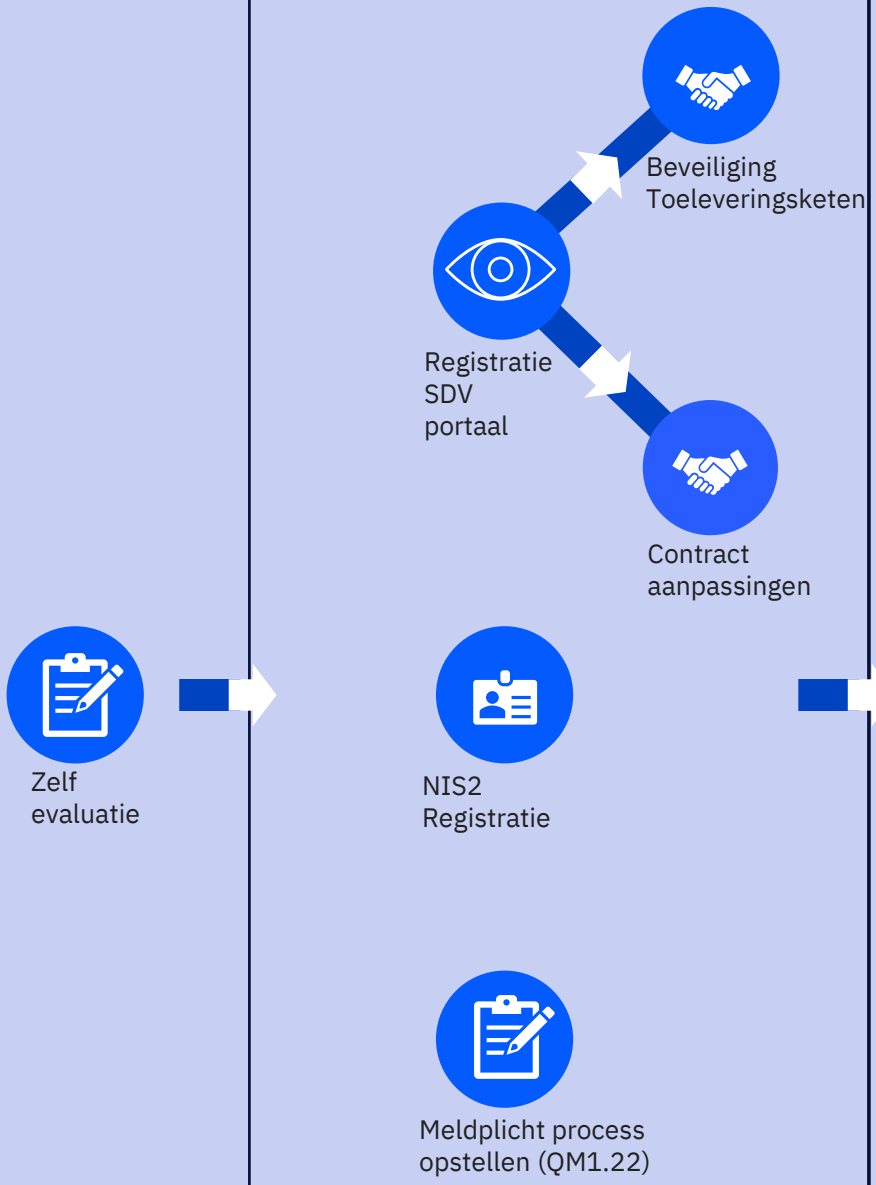
NIS2 als kans

Samen digitaal Veilig - Toeleveringsketen

De beveiliging van de toeleveringsketen is verplicht

- Dit kost (veel) tijd.
- Leveranciers hebben ook tijd nodig voor de “opgelegde” maatregelen.
- Hiervoor is de procurement/Inkoop afdeling is benodigd.
- De IT-afdeling kan parallel de eigen scope oppakken.
- Dit is een verplicht onderdeel voor NIS2-plichtigen.
- Dit is een verplicht onderdeel, ook voor de ISO27001 gecertifieerden.
- Dit is onderdeel van het NIS2-QM10.
- Wij kunnen hier middels een workshop bij helpen.





- Begin pragmatisch (overweeg later hierbij een Risico analyse).
- Voeg een QM toe aan het SDV-portaal, start met invullen van bestaande informatie.
- Start met de zaken die je zelf kunt doen.
- Betrek een partner bij de zaken, welke je niet zelf kunt/wilt doen.

QM10 QM20 QM30

- **QM10:** Wanneer er niets is en geen verplichting is.
- **QM20:** Wanneer de ambitie hoger ligt dan QM10.
- **QM30:** Wanneer er al een ISO27001 aanwezig is.

- Organisatorische, Mensgerichte, Fysieke, Technologische, (+ OT en IT) maatregelen
- Gericht op Mens, Proces, Techniek
- Beleidstukken, processen, technische maatregelen

- Geen idee of NIS2 op ons van toepassing is.

- Plichtig, maar nog zoekende wat te doen.
- Plichtig, bezig met behalen van QM.
- Plichtig en ISO 27001-gecertificeerd.

- Niet plichtig, maar verwachten wel actie via leveranciers.

NIS2 als kans

NIS2 Quality Mark

	Basic	Substantial	High
Organisatorische beheersmaatregelen	8	14	24
Mensgerichte beheersmaatregelen	3	3	7
Fysieke beheersmaatregelen	1	3	4
Technologische beheersmaatregelen	5	7	13
OT- beheersmaatregelen		5	8
IT- beheersmaatregelen		4	11
	17	36	67

NIS2-QM10
Basic

- Organisatorische controlemaatregelen
- Mensgerichte managementmaatregelen
- Fysieke beheersmaatregelen
- Technologische beheersmaatregelen

NIS2-QM20
Substantial

- Organisatorische controlemaatregelen
- Mensgerichte managementmaatregelen
- Fysieke beheersmaatregelen
- Technologische beheersmaatregelen
- OT-managementmaatregelen
- IT-managementmaatregelen

NIS2-QM30
High

- Organisatorische controlemaatregel
- Mensgerichte managementmaatregelen
- Fysieke beheersmaatregelen
- Technologische beheersmaatregelen
- OT-managementmaatregelen
- IT-managementmaatregelen

NIS2 QUALITY MARK

- QM10: Start hier, wanneer er niet is en geen verplichting is.
- QM20: Start hier, wanneer de ambitie hoger ligt dan QM10.
- QM30: Start hier, wanneer er al een ISO27001 aanwezig is.

- Begin pragmatisch (overweeg later hierbij een Risico analyse).
- Voeg QM toe aan het SDV-portaal, start met invullen van bestaande informatie.
- Start met de zaken die je zelf kunt doen.
- Betrek een partner bij de zaken, welke je niet zelf kunt /wilt doen.

Basic

Dit niveau is vergelijkbaar met wat de overheid hanteert als basis voor cybersecurity. Uitermate geschikt voor veel mkb-bedrijven.

Substantial

Dit niveau is geschikt voor bedrijven die een substantieel risico vormen voor hun klant. Een hack geeft last maar de impact is gemiddeld.

High

Dit niveau is voor leveranciers die een hoog risico vormen voor hun klant als ze niet meer leveren. Een hack heeft een stevige impact op de organisatie.

ISO - NEN

ISO en/of NEN normering is raadzaam als er met een leverancier gewerkt wordt die een extreem hoog risico vormt. Bij een hack ligt het bedrijf direct stil.

NIS2 als kans

GAP

NIS2 met IS27001

Met een ISO27001 certificering, is een goede basis gelegd voor richting NIS2 compliance, maar het is nog niet genoeg.

- Registratieplicht
- Meldplicht
- Opleiding directie
- OT Security
- Zorgplicht richting de leveranciersketen

Zelf evaluatie

NIS2 Registratie

Registratie SDV portaal

Beveiliging Toeleveringsketen

Contract aanpassingen

Meldplicht process opstellen (QM1.22)

- Begin pragmatisch (overweeg later hierbij een Risico analyse).
- Voeg een QM toe aan het SDV-portaal, start met invullen van bestaande informatie.
- Start met de zaken die je zelf kunt doen.
- Betrek een partner bij de zaken, welke je niet zelf kunt/wilt doen.

QM10 QM20 QM30

- **QM10:** Wanneer er niets is en geen verplichting is.
- **QM20:** Wanneer de ambitie hoger ligt dan QM10.
- **QM30:** Wanneer er al een ISO27001 aanwezig is.

- Organisatorische, Mensgerichte, Fysieke, Technologische, (+ OT en IT) maatregelen
- Gericht op Mens, Proces, Techniek
- Beleidstukken, processen, technische maatregelen

Cyber beveiligingswet Q3 2025

- Geen idee of NIS2 op ons van toepassing is.

- Plichtig, maar nog zoekende wat te doen.
- Plichtig, bezig met behalen van QM.
- Plichtig en ISO 27001-gecertificeerd.

- Niet plichtig, maar verwachten wel actie via leveranciers.

- Plichtig en QM30-gecertificeerd.

Zelf evaluatie

- Geen idee of NIS2 op ons van toepassing is.

Beveiliging Toeleveringsketen

Registratie SDV portaal

Contract aanpassingen

NIS2 Registratie

Meldplicht process opstellen (QM1.22)

- Plichtig, maar nog zoekende wat te doen.
- Plichtig, bezig met behalen van QM.
- Plichtig en ISO 27001-gecertificeerd.

- Begin pragmatisch (overweeg later hierbij een Risico analyse).
- Voeg een QM toe aan het SDV-portaal, start met invullen van bestaande informatie.
- Start met de zaken die je zelf kunt doen.
- Betrek een partner bij de zaken, welke je niet zelf kunt/wilt doen.

QM10 QM20 QM30

- **QM10:** Wanneer er niets is en geen verplichting is.
- **QM20:** Wanneer de ambitie hoger ligt dan QM10.
- **QM30:** Wanneer er al een ISO27001 aanwezig is.

- Organisatorische, Mensgerichte, Fysieke, Technologische, (+ OT en IT) maatregelen
- Gericht op Mens, Proces, Techniek
- Beleidstukken, processen, technische maatregelen

- Niet plichtig, maar verwachten wel actie via leveranciers.

Cyber beveiligingswet Q3 2025

- Plichtig en QM30-gecertificeerd.

- Continue proces
- Evalueren, verbeteren
- Riscoanalyse

- Alle organisaties

NIS2 als kans

Security is een werkwoord

Security is een continu proces

- Het beveiligen van de IT-omgeving is geen eenmalige activiteit, het is geen set-and-forget.
- QM10 -> QM20 -> QM30 -> … ISO27001
- Toevoegingen op de wetsdocumenten (middels de Algemene Maatregelen van Bestuur)
- Security = Continue proces
- Technieken, voor aanval en verdediging, zullen telkens veranderen net als de eisen voor security vanuit de organisatie, als vanuit wet & regelgeving
- Na het leggen van een basis, is het van belang de basis te behouden of te verbeteren en stilstand te voorkomen (stilstand is achteruitgang).

VRAGEN?

The people who power *your* possible

Meer weten?
Neem contact op met Ekco!

info_nl@ek.co

www.ek.co

+31 88 070 0600

Landjuweel 20, Veenendaal

6 mei 2025