The people who power your possible ...

NIS2 Groepsdeal

19 maart 2026

Ekco

Even voorstellen

Ekco & Samen Digitaal Veilig

Laurens Noortman
Ekco

Henk Bijsterbosch
Samen Digitaal Veilig

Agenda

1. Huishoudelijke mededelingen
2. Waarom dit webinar
3. Aanbieding voor relaties
4. Rol van Ekco in dit traject
5. Presentatie SDV
6. Recap
7. Vragen en afronding

NIS2

Relevantie van dit webinar

Waarom, groepsdeal en rol van Ekco

- **Waarom**
  - NIS2 handhaving is nu actueel (audits)
  - 2026 hét jaar van naleving
  - Bestuurders aansprakelijk; cyberrisico wordt juridische verantwoordelijkheid

- **Groepsdeal**
  - Meeste Ekco relaties hebben inmiddels aanbieding ontvangen
  - Financieel voordeel en **audit garantie in 2026**
  - Accountmanager neemt contact met je op over vervolg

- **Rol van Ekco**
  - Vertalen NIS2-eisen naar concrete maatregelen


EKCO
Samen
Digitaal
Veilig
NIS2 Cyberbeveiligingswet
Een wet met grote gevolgen

Samen Digitaal Veilig

MKB Nederland

VNO NCW

IVBB
Instituut voor Verenigingen Branches en Beroepen

Samen Digitaal Veilig

SDV is het grootste NIS2-platform van Nederland. Het is opgezet voor en door meer dan 100 samenwerkende brancheorganisaties om ruim 200.000 bedrijven en organisaties te ondersteunen bij deze nieuwe wet.

NIS2 Cyberbeveiligingswet

Ca. 10.000 bedrijven en organisaties vallen direct onder de wet.

Indirect krijgen ca. 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. Dat kan via NIS2-certificering.

Samen Digitaal Veilig

Direct of indirect...

Alle bedrijven en organisaties krijgen te maken met de NIS2 Cyberbeveiligingswet. Ook al val je er niet zelf niet direct onder de wet dan krijg je er toch mee te maken. Sommige bedrijven hebben tot recent gedacht dat het hen niet ging raken. Dit was een misverstand.

Samen Digitaal Veilig

Wat zegt de Toezicht houder?

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.

Samen
Digitaal
Veilig

Deze wetgeving heeft een domino-effect

Bij elke nieuwe wet zijn er effecten.

Samen
Digitaal
Veilig

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.

Samen Digitaal Veilig

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?

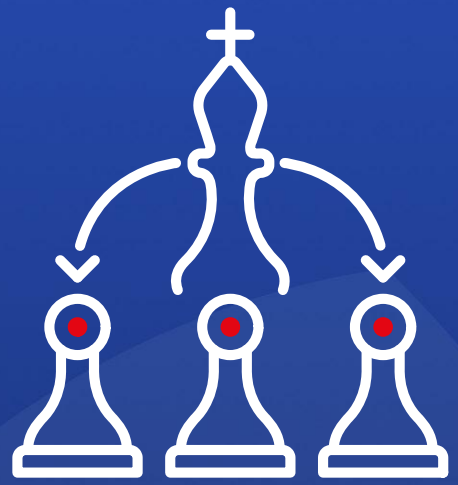
Samen Digitaal Veilig

Banken en Accountants laten cybersecurity zwaarder meewegen

Steeds vaker nemen banken digitale veiligheid mee in hun risicoanalyse. Bedrijven zonder aantoonbare cybersecurity krijgen moeilijker financiering.

Accountants gaan strenger toetsen op cyberrisico's en kunnen in de jaarrekening of het jaarverslag bevindingen komen over tekortkomingen.

Samen Digitaal Veilig



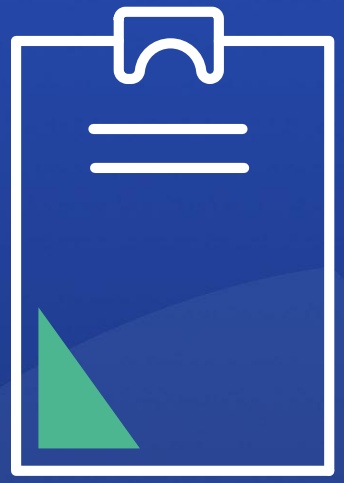
Je Cybersecurity op orde telt bij bedrijfsovername

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

Cyberverzekeringen stellen strengere eisen

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

Samen Digitaal Veilig



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.

Samen Digitaal Veilig

Certificering wordt een ‘license to operate’

Digitale veiligheid is een ook 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.

Samen Digitaal Veilig

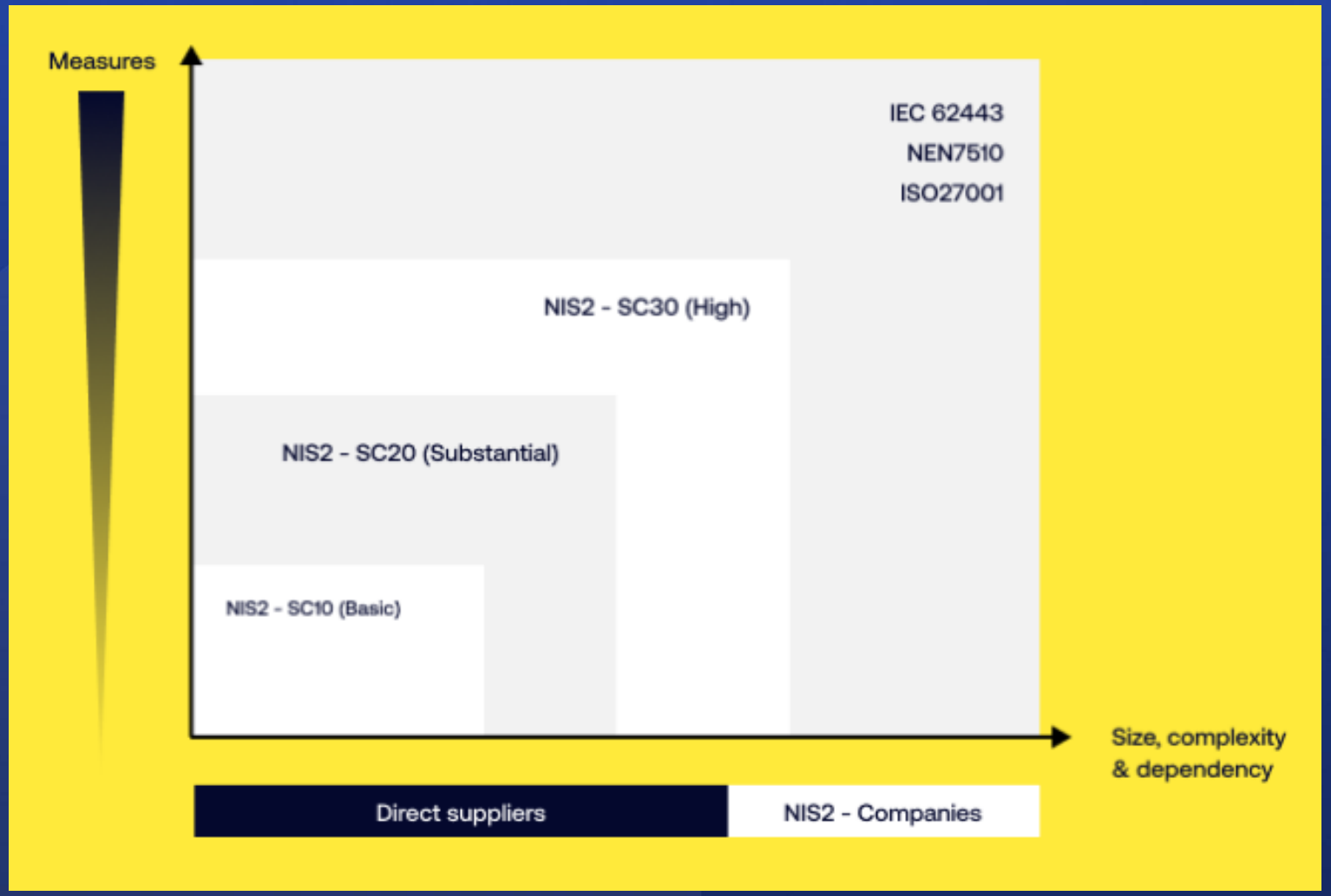
NIS2-certificering is je digitale brandblusser

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

Samen Digitaal Veilig

De norm voor de toeleveringsketen



NIS2 Supply Chain kent 3 niveaus, afgestemd op het belang en de omvang van de organisatie

- NIS2-SC10 (Basic)
- NIS2-SC20 (Substantial)
- NIS2-SC30 (High)

Samen Digitaal Veilig

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.

Samen Digitaal Veilig

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

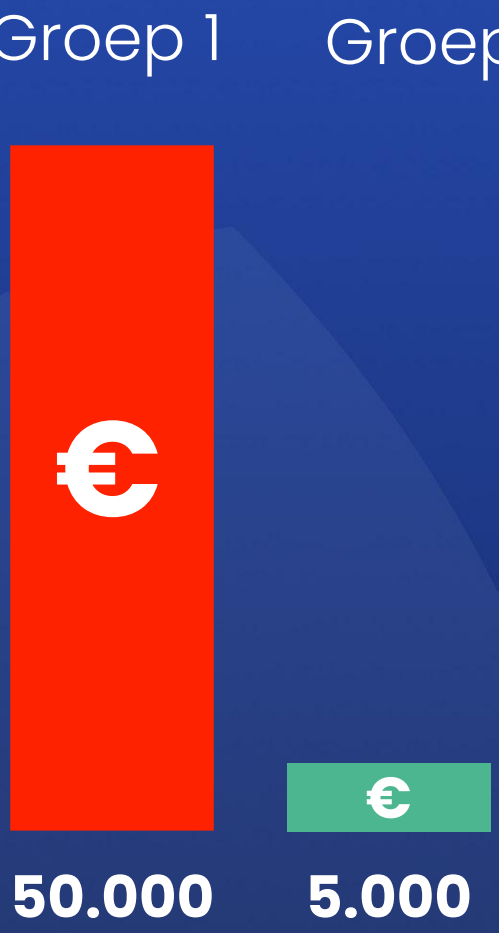
NIS2 Supply Chain certificate:

Company ABC

for completing the NIS2 Supply Chain Audit successfully

Dr. D.P. Noordhoek RAE
Director-Secretary
Foundation for Quality & Innovation

#2738491039



Indicatie van investering voor certificering

8.000-10.000 bedrijven en organisaties in Groep 1

50.000-100.000 bedrijven en organisaties in Groep 2.

Samen Digitaal Veilig

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.

De logica van certificering

Neem de logische stap en ga ervoor zorgen dat je kunt bewijzen dat je cyber security op orde is.

Haal je NIS2 Supply Chain Certificaat. De norm voor NIS2.

Samen Digitaal Veilig

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

Samen Digitaal Veilig

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

← Maatregelenlijsten / NIS2 Supply Chain

NIS2-SC10 BASIC

Overzicht antwoorden

VOORTGANG 41%

Beveiliging van apparaten 4.1

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.

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.

Deze maatregel is aangepast volgens de NIS2 Supply Chain-norm versie 3.2 (15-12-2025). Een overzicht van de laatste wijzigingen vind je op de Startpagina bij SDV-updates.

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 voorbeelden van regels die je kunt opstellen.

HULPMIDDELEN

- Toelichtingsdoc1_Wat zijn gebruikersapparaten
- Toelichtingsdoc2_Voorbeelden technische veiligheidsmaatregelen
- Toelichtingsdoc3_Voorbeelden betrekken gebruikers

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.

HULPMIDDELEN

- Toelichtingsdoc1_Wat zijn gebruikersapparaten
- Toelichtingsdoc2_Voorbeelden technische veiligheidsmaatregelen

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

← Vragenlijst

NIS2-SC10 BASIC

Antwoorden overzicht in PDF

Informatiebeveiligingsbeleid 1.2

- ✓ Is er een informatiebeveiligingsbeleid ontwikkeld en is dit goedgekeurd en gecommuniceerd door de directie?
- ⚠ Is het beleid gepubliceerd, is het bekend bij het personeel en relevante belanghebbenden en wordt het regelmatig beoordeeld?

Verantwoordelijkheden 1.3

- ✓ Zijn de taken en verantwoordelijkheden voor cybersecurity duidelijk gedefinieerd en toegewezen?
- ✓ Is er een primaire persoon of een team verantwoordelijk voor de cybersecurity van de gehele organisatie?

Overzicht van informatie 1.6.1

- ✓ Is er een overzicht van bedrijfsinformatiecategorieën (informatieregister) opgesteld om de informatie van de organisatie vast te leggen en is dit volledig, nauwkeurig en actueel?
- ✓ Is er een duidelijke eigenaar of beheerder aangewezen voor de informatie in de verschillende categorieën van het overzicht?

ICT-bedrijfsmiddelen 1.6.2

- ✓ Zijn de ICT-bedrijfsmiddelen in de organisatie in kaart gebracht?
- ⚠ Is er een up-to-date inventarisatielijst van alle ICT-bedrijfsmiddelen in de organisatie en is er een eigenaar/beheerder en, indien van toepassing, een gebruiker – geïdentificeerd voor elk ICT-bedrijfsmiddel?

HET INLEVEREN VAN BEDRIJFSMIDDELEN NA GEBRUIK

Checklist

VOORBEELD VAN EEN UITGEWERKTE CHECKLIST

Een checklist voor het inleveren van bedrijfsmiddelen na gebruik kan dienen als een handige tool voor zowel de medewerker die vertrekt als de organisatie. Hieronder zie je een voorbeeld van een uitgewerkte checklist voor het inleveren van bedrijfsmiddelen na gebruik bij een IT-bedrijf.

Checklist voor het inleveren van bedrijfsmiddelen na gebruik bij [IT-bedrijf]

Persoonlijke gegevens

- ❑ Naam van de medewerker
- ❑ Afdeling
- ❑ Laatste werkdag

Apparatuur en elektronica

- ❑ Laptop (inclusief lader en eventuele extra's zoals muizen of toetsenborden)
- ❑ Mobiele telefoon (inclusief oplader)
- ❑ Externe harde schijven of USB-sticks
- ❑ Headset / Oortjes

Toegangsmiddelen

- ❑ Toegangspas / ID-kaart
- ❑ Parkeerkaart
- ❑ Sleutels (gebouw, kluis, kantoor)

Software en data

Samen Digitaal Veilig
Digitale veiligheid voor zakelijk Nederland

VOORBEREIDING EN OPTIMALISATIE VAN ICT VOOR CONTINUE BEDRIJFSVOERING

ICT-continuïteitsplan inclusief voorbeeld

Als de ICT-continuïteitseisen vastgesteld zijn, kun je continuïteitsstrategieën ontwikkelen die de situaties voor, tijdens en na een verstoring in overweging nemen.

Opbouw ICT-continuïteitsplan

Bij het opstellen van een ICT-continuïteitsplan kun je de volgende opbouw gebruiken:

1. **Achtergrond & doel**
- Beschrijving van de organisatie en de primaire bedrijfsprocessen.
- Doelstellingen en de reikwijdte van het ICT-continuïteitsplan.

2. **Risicoanalyse**
- Identificatie van kritieke bedrijfsprocessen en bijbehorende ICT-systemen.
- Analyse van potentiële bedreigingen en hun impact op de ICT-infrastructuur.

3. **Strategieën voor ICT-continuïteit**
- Backup- en herstelstrategieën.
- Uitwijkstrategieën voor noodsituaties.

4. **Maatregelen**
- Redundantie van kritieke systemen.
- Data back-up procedures en frequentie.
- Plannen voor regelmatig onderhoud en updates.

Redundantie bij kritieke systemen houdt in dat er een extra systeem klaarstaat om het over te nemen als het hoofdsysteem uitvalt. Zo zorg je ervoor dat alles blijft draaien, zelfs als er iets misgaat.

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

Toeleveranciers/ relaties

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

Ondersteunende documenten

20 Toeleveranciers/ relaties

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

Zoeken

Leverancier	Risico-inventarisatie	Risicoprofiel	E.R.I.	NIS2 Cyber Score	Certificaat	Notitie	Status	Bewerk
Paree	RI nog doen	Niet ingesteld	8.7	Uitnodigen			Niet gestart	
Meulenbaan Consultancy	RI gereed (Advies: Hoog)	Substantieel	8.4	★★★★★ 5,6			Dringend actie	
Eneco	RI bezig	Substantieel	9	Herinneren			Gereed	
Heroso	RI bezig	Niet ingesteld	8.4	Uitnodigen			Gereed	
Mepaco	RI nog doen	Niet ingesteld	8.8	Uitnodigen			Bezig	
Feenstra CTAC	RI nog doen	Niet ingesteld	9.4	Uitnodigen			Gereed	
Broekman Software	RI nog doen	Niet ingesteld	9.4	Uitnodigen			Dringend actie	
Alle kleine levs geen risico toch	RI bezig	Niet ingesteld	-	Uitnodigen			Niet gestart	
ALLE KLEINE LEVS GEEN RISICO	RI nog doen	Niet ingesteld	-	Bezig met invullen			Niet gestart	
ALLE GROTE	RI bezig	Niet ingesteld	-	Uitnodigen			Niet gestart	

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:

- **Wacht niet af: Start nu met je eigen NIS2-SC traject en blijf onderdeel van de (toeleverings)keten**
- **Ekco & ICT & SDV ondersteunen**
- **In 2026 ontstaat auditoren schaarste, met de groepsdeal kun je een concurrerend voordeel creëren**

Samen Digitaal Veilig

Wij – Ekco en Samen Digitaal Veilig – gaan je helpen!

EKCO

Samen Digitaal Veilig

Vragen?

info_nl@ek.co