GIDS

De complete gids voor cybersecurity risicoanalyse

Methodieken, kosten, NIS2-verplichting, valkuilen en selectiecriteria. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

71% van alle Nederlandse bedrijven voert geen periodieke risicoanalyse uit. Tegelijkertijd maakt NIS2 het wettelijk verplicht. De kloof is enorm.

71%

van alle Nederlandse bedrijven voert geen periodieke cybersecurity risicoanalyse uit

CBS Cybersecuritymonitor 2024 [1]

EUR 270K

Gemiddelde schade per cyberincident voor Nederlands MKB

ESET/Hallo [2]

87%

van grote bedrijven (250+ fte) voert wel een periodieke risicoanalyse uit

CBS Cybersecuritymonitor 2024 [1]

23%

van micro-bedrijven (2--10 fte) doet het -- de rest investeert blind

CBS Cybersecuritymonitor 2024 [1]

Art. 21

NIS2 zorgplicht: risicoanalyse staat op de eerste plaats van 10 verplichte maatregelen

NIS2 Richtlijn [3]

EUR 2.500

Startprijs risicoanalyse voor micro-bedrijf (2--10 fte)

Marktindicatie [4]

1 op 4

MKB-bedrijven werd in 2024 slachtoffer van een datalek

W3E [5]

EUR 20M

Maximale AVG-boete of 4% wereldwijde omzet bij niet-naleving

AVG [6]

1. Wat is een cybersecurity risicoanalyse?

Een cybersecurity risicoanalyse is een systematische evaluatie van dreigingen, kwetsbaarheden en potentiele impact op de informatiesystemen en bedrijfsprocessen van je organisatie.

Het doel: risico's identificeren, prioriteren en beheersmaatregelen bepalen. Niet alles tegelijk beveiligen, maar je budget en aandacht richten op waar het risico het grootst is. Een risicoanalyse beantwoordt de vraag: "Wat kan er misgaan en hoe erg is dat?" [7]

WAT LEVERT HET OP?

- **Risico-inventarisatie** -- Overzicht van alle geidentificeerde risico's
- **Risicoregister** -- Classificatie per risico op waarschijnlijkheid en impact
- **Risicomatrix** -- Visuele weergave van risico's (heatmap)
- **Maatregelplan** -- Concrete beheersmaatregelen per risico met prioritering
- **Quick wins** -- Direct uitvoerbare verbeteringen
- **Management-samenvatting** -- Bestuurlijke rapportage voor directie [8]

Een risicoanalyse is de **eerste stap** in elk cybersecurity-traject. Zonder analyse investeer je blind -- mogelijk te veel in lage risico's en te weinig in hoge risico's. Het is de basis voor alle andere security-beslissingen: welke tools je koopt, welke processen je inricht, waar je budget naartoe gaat.

2. Waarom is het belangrijk?

NIS2 maakt risicoanalyse wettelijk verplicht. Maar ook zonder wetgeving: zonder risicoanalyse investeer je blind in cybersecurity.

DE CIJFERS

71% van alle Nederlandse bedrijven voert geen periodieke risicoanalyse uit. Bij micro-bedrijven (2--10 fte) is dat 77%. Tegelijkertijd werd 1 op de 4 MKB-bedrijven in 2024 slachtoffer van een datalek [1] [5]. De gemiddelde schade per cyberincident voor Nederlands MKB bedraagt EUR 270.000 [2].

NIS2 MAAKT HET VERPLICHT

De Cyberbeveiligingswet (NIS2-implementatie) treedt naar verwachting in Q2 2026 in werking. Risicoanalyse staat op de eerste plaats van de 10 verplichte zorgplichtmaatregelen (Artikel 21 lid 2 sub a). Voor duizenden Nederlandse organisaties wordt het daarmee een wettelijke verplichting [3].

BASIS VOOR ALLE SECURITY-BESLISSINGEN

Een risicoanalyse bepaalt waar je budget naartoe gaat. Zonder analyse koop je tools die misschien niet bij je risico's passen, investeer je in training die het verkeerde gedrag adresseert, of sluit je een cyberverzekering af die de verkeerde risico's dekt. Met een analyse investeer je gericht: budget waar het risico het grootst is [9].

EUR 5.000

Investering in een risicoanalyse voor klein MKB

Marktindicatie [4]

EUR 270K

Gemiddelde schade per cyberincident -- 54x de investering

ESET/Hallo [2]

> **Verzekeraars eisen het steeds vaker**
>
> Cyberverzekeraars vragen steeds vaker om een recente risicoanalyse als voorwaarde voor acceptatie. Zonder analyse betaal je een hogere premie of word je geweigerd. De risicoanalyse betaalt zichzelf terug via lagere premies, gerichte investeringen en vermeden schade [10].

3. Hoe werkt het?

Een risicoanalyse volgt een gestructureerd proces. Het NCSC-stappenplan is de standaard voor Nederlandse organisaties.

HET PROCES IN 4 STAPPEN (NCSC-MODEL)

1 Kroonjuwelen identificeren

Bepaal welke assets beschermd moeten worden: klantdata, financiele gegevens, unieke ontwerpen, bedrijfsprocessen. Wat zijn de systemen en data die je organisatie niet kan missen? [11]

2 Risico's identificeren

Inventariseer dreigingen via incident-historie, regelgeving (AVG, NIS2), branchespecifieke dreigingen en externe adviseurs. Denk aan ransomware, phishing, insider threats, supply chain-aanvallen en menselijke fouten.

3 Risico's analyseren

Beoordeel per risico de waarschijnlijkheid en de impact. Dit kan kwalitatief (laag/medium/hoog) of kwantitatief (percentages en bedragen). Plaats risico's in een risicomatrix.

4 Maatregelen bepalen

Kies per risico een strategie: accepteren (lage kans + lage impact), mitigeren (maatregelen treffen), overdragen (cyberverzekering) of stoppen (activiteit beeindigen) [11].

UITGEBREID PROCES (6 STAPPEN)

STAP	WAT DOE JE
1. Stakeholders in kaart	Betrek IT, management, operations -- een risicoanalyse doe je niet alleen [12]
2. Processen identificeren	Niet alleen systemen maar ook werkplekken, apparatuur, essentiele medewerkers
3. Maximale uitvaltijd bepalen	Hoelang voordat het echt kritiek wordt als processen stilvallen?
4. Klantimpact beoordelen	Directe klantgevolgen en reputatieschade inschatten
5. Herstelkosten berekenen	Niet alleen de oplossing, maar ook omzetverlies en bijkomende schade

STAP	WAT DOE JE
6. Prioriteren	Bepaal welke procesverstoringen de grootste impact hebben

METHODIEKEN

METHODIEK	TYPE	GESCHIKT VOOR
ISO 27005	Internationaal framework	Alle organisaties, integreert met ISO 27001 [13]
NIST CSF	Framework (VS)	Alle organisaties, praktisch gericht
NCSC Basisprincipes	Nederlandse richtlijn	MKB, praktische basisbeveiliging
MAPGOOD	Nederlandse dreigingsclassificatie	Alle organisaties, 7 categorieen
NOREA CSA/ICR	Nederlandse assessment tool	IT-auditors, gratis beschikbaar [14]
BIV-classificatie	Nederlands classificatiemodel	Alle organisaties (Beschikbaarheid, Integriteit, Vertrouwelijkheid)
FAIR	Kwantitatief model	Volwassen organisaties, financiele risicokwantificering

TIP

Voor MKB is de NCSC Basisprincipes-aanpak het meest praktisch. Begin met de gratis zelfscan van het Digital Trust Center (9 vragen, bepaalt je risicoklasse) en gebruik dat als startpunt voor een externe risicoanalyse.

4. Wat kost het?

De kosten van een risicoanalyse hangen af van je bedrijfsgrootte, complexiteit en gewenste diepgang. Dit zijn de indicaties voor de Nederlandse markt.

PROJECTKOSTEN PER SEGMENT

BEDRIJFSGROOTTE	GESCHATTE KOSTEN	DOORLOOPTIJD
Micro (2--10 fte)	EUR 2.500--5.000	1--2 weken
Klein (10--50 fte)	EUR 5.000--15.000	2--4 weken
Middelgroot (50--250 fte)	EUR 15.000--35.000	4--8 weken
Groot (250+ fte)	EUR 35.000--75.000+	8--16 weken [4]

CONSULTANT TARIEVEN

TYPE	TARIEF
Uurtarief cybersecurity consultant (zzp)	~EUR 114/uur [15]
Dagprijs senior security consultant	EUR 800--1.200/dag
Dagprijs specialist (CISO-niveau)	EUR 1.200--1.800/dag

SELF-ASSESSMENT VS EXTERN

ASPECT	SELF-ASSESSMENT	EXTERNE RISICOANALYSE
Kosten	Laag (gratis tools beschikbaar)	EUR 2.500--75.000+
Diepgang	Beperkt, oppervlakkig	Grondig, gedetailleerd
Objectiviteit	Beperkt (blinde vlekken)	Hoog (onafhankelijk perspectief)
Doorlooptijd	1--2 uur	1--16 weken
Geschikt voor	Eerste orientatie, bewustwording	Compliance, NIS2, certificering [16]

GRATIS SELF-ASSESSMENT TOOLS (NL)

- **NCSC/Digital Trust Center Zelfscan** -- 9 vragen, bepaalt risicoklasse [16]
- **NOREA ICR** -- Inherente Cyber Risicoanalyse, gratis spreadsheet [14]

> **ROI van een risicoanalyse**
>
> Een investering van EUR 5.000 versus een gemiddelde schade van EUR 270.000 per incident. De ROI-ratio is 18:1 tot 108:1 (kosten analyse vs vermeden schade). Daarnaast: lagere cyberverzekeringspremies, gerichte security-investeringen en NIS2-compliance [9].

5. Waar moet je op letten?

Niet elke risicoanalyse is gelijk. Deze selectiecriteria en vragen helpen je de juiste aanpak en partij te kiezen.

SELECTIECRITERIA

CRITERIUM	WAAROM HET ERTOE DOET
Ervaring in jouw sector	Sectorspecifieke dreigingen en regelgeving vereisen domeinkennis
Methodiek	Welk framework wordt gehanteerd (ISO 27005, NIST CSF, NCSC)? Past het bij je doelstelling?
Scope en diepgang	Quickscan of volledige analyse? Alleen technisch of ook organisatorisch en menselijk?
Deliverables	Krijg je een risicomatrix, maatregelplan en management-samenvatting? Of alleen een rapport?
Onafhankelijkheid	Is de consultant onafhankelijk of verkoopt hij tegelijkertijd security-producten?
Certificeringen	CISSP, CISM, ISO 27001 Lead Auditor, NOREA RE -- kwaliteitsborging van de consultant
NIS2-kennis	Kan de consultant de risicoanalyse koppelen aan NIS2-zorgplichtmaatregelen?
Follow-up ondersteuning	Helpt de consultant ook bij implementatie van maatregelen of is het een eenmalig rapport? [7]

10 VRAGEN AAN EEN CONSULTANT

1. Welke methodiek gebruikt je voor de risicoanalyse en waarom die?
2. Hoe bepaal je de scope -- analyseer je ook processen en mensen, of alleen IT?
3. Welke deliverables krijg ik concreet (risicomatrix, maatregelplan, management-samenvatting)?
4. Heb je ervaring in mijn sector en ken je de sectorspecifieke dreigingen?
5. Hoe koppel je de risicoanalyse aan NIS2-zorgplichtmaatregelen?
6. Wat is de doorlooptijd en hoeveel tijd vraagt het van mijn team?
7. Bied je ook ondersteuning bij de implementatie van de aanbevolen maatregelen?
8. Hoe ga je om met de vertrouwelijkheid van de bevindingen?
9. Wat zijn de kosten en wat zit er precies bij in?

10. Kan ik referenties spreken van vergelijkbare organisaties?

> **LET OP: RAPPORT IN DE LA**
>
> Het grootste risico van een risicoanalyse is dat het rapport in de la belandt. Zonder follow-up, implementatie van maatregelen en periodieke herziening is de analyse verspild geld. Spreek vooraf af hoe de aanbevelingen worden opgepakt.

6. Veelgemaakte fouten

Deze tien valkuilen ondermijnen de waarde van je risicoanalyse.

1. Eenmalig in plaats van periodiek

Een risicoanalyse is geen eenmalige exercitie. Risico's veranderen continu door nieuwe dreigingen, technologie en organisatiewijzigingen. Plan minimaal jaarlijks een herziening, plus een extra analyse bij significante veranderingen [3].

2. Geen management-betrokkenheid

Zonder commitment van directie wordt de analyse niet serieus genomen en worden maatregelen niet geimplementeerd. De risicoanalyse moet een bestuurlijk proces zijn, niet alleen een IT-project [17].

3. Te technisch

Focus alleen op IT terwijl menselijke en organisatorische risico's worden vergeten. Social engineering, processen, fysieke beveiliging en leveranciersrisico's zijn minstens zo relevant. Een goede analyse dekt mensen, processen en techniek [7].

4. Over-scoping

Alles tegelijk willen analyseren overweldigt teams en levert rapporten op die te breed zijn om actie op te ondernemen. Begin met je kroonjuwelen en breid geleidelijk uit.

5. Ketenrisico's onderschatten

Leveranciers, cloudplatformen en supply chain-partners zijn vaak de zwakste schakel. NIS2 eist expliciet dat je ketenbeveiliging meeneemt in je risicoanalyse [3].

6. Compliance als einddoel

Een audit doorstaan garandeert geen veiligheid. Focus op daadwerkelijke risicobeheersing met compliance als bijproduct -- niet andersom [17].

7. Geen monitoring na analyse

Zonder doorlopende monitoring worden nieuwe dreigingen en kwetsbaarheden gemist. Een risicoanalyse is een momentopname -- de wereld verandert de dag erna.

8. Slechte communicatie

Bevindingen bereiken niet alle relevante stakeholders. Zorg voor een management-samenvatting naast het technische rapport. Verschillende doelgroepen hebben verschillende informatie nodig.

9. Risico's niet goed identificeren

Onvoldoende kennis van dreigingen leidt tot blinde vlekken. Gebruik actuele dreigingsinformatie (NCSC, sectorale CSIRTs) en externe expertise om je dreigingsbeeld compleet te maken [11].

10. Rapport in de la

Geen follow-up, geen implementatie, geen review-cycli. De analyse wordt "shelfware". Spreek vooraf af: wie pakt welke maatregel op, met welk budget, op welke deadline?

TIP

Koppel elke geidentificeerde maatregel aan een eigenaar, een deadline en een budget. Een risicoanalyse zonder implementatieplan is een duur rapport.

7. NIS2: risicoanalyse verplicht

De Cyberbeveiligingswet (NIS2-implementatie) maakt risicoanalyse maatregel nummer 1 van de 10 verplichte zorgplichtmaatregelen.

DE 10 NIS2 ZORGPLICHTMAATREGELEN

#	MAATREGEL	TOELICHTING
1	**Risicoanalyse en beveiliging informatiesystemen**	De basis: identificeer, analyseer en behandel risico's [3]
2	Toegangsbeleid	Rolgebaseerd, MFA, assetbeheer
3	Bedrijfscontinuiteit	BCP met backupprocedures
4	Incidentafhandeling	Detectie, mitigatie, 24-uurs meldplicht
5	Cyberhygiene	Basisbeveiliging en awareness
6	Netwerk- en systeembeveiliging	Patchmanagement, change management
7	Ketenbeveiliging	Leveranciersbeheer en contracten
8	Cryptografie	Versleutelingsbeleid
9	Veilige communicatie	MFA, VPN
10	Effectiviteitstesting	Periodieke beoordeling van maatregelen

FREQUENTIE EN AANPAK

- **Jaarlijks** een risicoanalyse uitvoeren is de aanbeveling van het Digital Trust Center
- **Bij significante wijzigingen** (nieuwe systemen, fusie, cloudmigratie) een extra analyse
- Een **beleidsplan risicoanalyse** vastleggen: frequentie, rollen, verantwoordelijkheden en risicoacceptatiecriteria [18]

WIE VALT ONDER NIS2?

TYPE	SECTOREN	DREMPEL
Essentiele entiteiten	Energie, transport, bankwezen, gezondheidszorg, drinkwater, digitale infrastructuur, overheidsdiensten	50+ medewerkers of EUR 10M+ omzet
Belangrijke entiteiten	Post/koeriersdiensten, afvalverwerking, voedselproductie, chemie, ICT-dienstverleners, onderzoek	50+ medewerkers of EUR 10M+ omzet [19]

SANCTIES

Essentiele entiteiten: tot EUR 10 miljoen of 2% wereldwijde jaaromzet. Belangrijke entiteiten: tot EUR 7 miljoen of 2% wereldwijde jaaromzet. Plus persoonlijke bestuurdersaansprakelijkheid [20].

> **RISICOANALYSE IS NIET OPTIONEEL**
>
> NIS2 maakt risicoanalyse wettelijk verplicht. Zonder actuele risicoanalyse kun je niet aantonen dat je aan de zorgplicht voldoet. De boetes zijn fors en de persoonlijke aansprakelijkheid van bestuurders is nieuw.

8. Risicoanalyse vs pentest vs audit vs gap-analyse

Vier instrumenten die vaak verward worden. Ze zijn complementair, niet uitwisselbaar.

ASPECT	RISICOANALYSE	PENTEST	SECURITY AUDIT	GAP-ANALYSE
Vraag	Wat kan er misgaan en hoe erg is dat?	Kunnen we daadwerkelijk binnenkomen?	Voldoen we aan de regels?	Waar staan we t.o.v. een norm?
Focus	Bedrijfsrisico's en impact	Technische kwetsbaarheden exploiteren	Compliance en beleid	Verschil huidige en gewenste situatie
Aanpak	Evaluatief, strategisch	Actief testen, hands-on	Onderzoekend, documentatie	Vergelijkend, normatief
Wie	Security consultant + management	Ethisch hacker / pentester	IT-auditor	Consultant / auditor
Output	Geprioriteerde risicolijst + maatregelen	Bewijs van exploiteerbaarheid	Compliance-rapport	Verbeterplan t.o.v. norm
Frequentie	Jaarlijks + bij wijzigingen	Jaarlijks of vaker	Jaarlijks of bij certificering	Eenmalig of periodiek [7]

Hoe verhouden ze zich?

Begin met een risicoanalyse. Die bepaalt waar pentests en audits nodig zijn. Een gap-analyse gebruik je om te meten hoe ver je bent richting een norm (ISO 27001, NIS2). Ze zijn complementair: de risicoanalyse is het startpunt, de rest volgt eruit.

KWALITATIEF VS KWANTITATIEF

ASPECT	KWALITATIEF	KWANTITATIEF
Schaal	Laag / Medium / Hoog	Getallen en percentages
Basis	Expert-oordeel, ervaring	Data, statistieken, modellen

ASPECT	KWALITATIEF	KWANTITATIEF
Snelheid	Sneller, goedkoper	Tijdsintensiever, duurder
Geschikt voor	Eerste orientatie, MKB	Financiele onderbouwing, enterprise
Voorbeeld	"Ransomware-risico = Hoog"	"Kans 15%, impact EUR 500.000, ALE = EUR 75.000" [16]

9. Trends 2025--2026

Drie ontwikkelingen die cybersecurity risicoanalyse de komende jaren veranderen.

1. NIS2 drijft massale adoptie

De Cyberbeveiligingswet maakt risicoanalyse verplicht voor duizenden Nederlandse organisaties. Dit creert een explosie in vraag naar zowel externe consultants als self-assessment tools. De markt verschuift van "nice to have" naar "wettelijk verplicht" [3].

2. AI-ondersteunde risicoanalyse

AI-tools automatiseren delen van het proces: asset discovery, dreigingsanalyse en risicoscoring. Dit maakt risicoanalyses sneller en goedkoper, waardoor ze toegankelijker worden voor MKB. Tegelijkertijd maakt AI de dreigingen complexer -- AI-gestuurde aanvallen vereisen een breder dreigingsbeeld [21].

3. Continue risicoanalyse vervangt jaarlijkse momentopnames

De traditionele jaarlijkse risicoanalyse wordt aangevuld met continue monitoring van het risicolandschap. Real-time dreigingsinformatie, geautomatiseerde vulnerability scanning en dynamische risicoscoring maken het mogelijk om risico's doorlopend te beoordelen in plaats van een keer per jaar. Voor MKB is de jaarlijkse analyse nog steeds het startpunt, maar de richting is duidelijk.

WAT BETEKENT DIT VOOR JOU?

De drempel om te starten met een risicoanalyse daalt (gratis tools, AI-ondersteuning, meer aanbieders), terwijl de noodzaak stijgt (NIS2-verplichting, complexere dreigingen, verzekeraars die het eisen). 2026 is het jaar om te beginnen -- of je huidige aanpak te professionaliseren.

10. Aan de slag

Een risicoanalyse is de eerste stap in je cybersecurity-traject. Drie acties die je vandaag kunt ondernemen.

1. Start met een zelfscan

Gebruik de gratis zelfscan van het Digital Trust Center (9 vragen, bepaalt je risicoklasse) als eerste orientatie. Het kost 15 minuten en geeft je een basis om het gesprek met een consultant te starten [16].

2. Plan een externe risicoanalyse

Vanaf EUR 2.500 voor een micro-bedrijf heb je een professionele risicoanalyse met risicomatrix, maatregelplan en management-samenvatting. Kies een consultant met ervaring in jouw sector en kennis van NIS2. Gebruik de 10 vragen uit hoofdstuk 5 om aanbieders te vergelijken [4].

3. Maak het periodiek

Plan de risicoanalyse jaarlijks in en voer een extra analyse uit bij significante veranderingen (nieuwe systemen, fusie, cloudmigratie). Koppel de resultaten aan je budget: de risicoanalyse bepaalt waar je geld naartoe gaat.

Bronnenlijst

[1] **CBS** -- Cybersecuritymonitor 2024: 71% voert geen risicoanalyse uit, 23% micro, 87% groot. cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024?onepage=true

[2] **ESET / Hallo** -- Cybercriminaliteit kost MKB EUR 270.000 per incident. hallo.eu/kennis/blogs/cybercriminaliteit-kost-mkb-euro-270-000-per-incident/

[3] **Legalz** -- NIS2-zorgplicht in 10 maatregelen: risicoanalyse op eerste plaats. legalz.nl/blog/nis2-zorgplicht

[4] **Marktindicatie** -- Geschatte projectkosten op basis van consultanttarieven en geschatte inzet. mijnzzp.nl/Beroep/756-Security-Specialist-(ICT)/Salaris-en-tarief

[5] **W3E** -- Wat kost een datalek echt? 1 op 4 MKB slachtoffer in 2024. w3e.nl/en/wat-kost-een-datalek-echt-alle-verborgen-kostenposten-op-een-rij/

[6] **AVG Compleet** -- AVG-boetes: max EUR 20M of 4% wereldwijde omzet. avg-compleet.nl/dit-zijn-de-boetes-en-reputatieschade-door-een-datalek/

[7] **Fortezza** -- Een goede risicoanalyse: definitie, verschil met pentest en audit. fortezza-cybersecurity.nl/een-goede-risicoanalyse/

[8] **Computest** -- Risk Assessment: deliverables en aanpak. computest.nl/nl/diensten/security/risk-assessment/

[9] **Safe Security** -- Measuring Cybersecurity ROI: framework voor 2026 decision-makers. safe.security/resources/blog/measuring-cybersecurity-roi-a-framework-for-2026-decision-makers/

[10] **NTNT** -- Wat kost goede cybersecurity voor een MKB? Verzekeraars eisen risicoanalyse. ntnt.nl/wat-kost-goede-cybersecurity-voor-een-mkb/

[11] **NCSC** -- Stappenplan risicoanalyse: kroonjuwelen, risico's, analyse, maatregelen. ncsc.nl/risicomanagement/stappenplan-risicoanalyse

[12] **Simac** -- Risicoanalyse in 6 stappen: stakeholders, processen, uitvaltijd. simac.com/nl/cybersecurity/blog/risicoanalyse-welke-cyberrisicos-loopt-jouw-organisatie

[13] **DigiTrust** -- Welke methodieken voor risicoanalyse? ISO 27005, NIST, FAIR. digitrust.nl/en/articles/what-methodologies-do-you-use-for-risk-analysis/

[14] **NOREA** -- Cyber Security Assessment & Inherente Cyber Risicoanalyse, gratis tools. norea.nl/uploads/bfile/e863236b-8e4e-4632-ad63-b62c0ac33bc3

[15] **MijnZZP / Knab** -- Uurtarief cybersecurity consultant ~EUR 114/uur. mijnzzp.nl/Beroep/756-Security-Specialist-(ICT)/Salaris-en-tarief

[16] **Digital Trust Center** -- Zelfscan en tools voor MKB. digitaltrustcenter.nl/tools

[17] **CyberDB / Atlant Security** -- Common pitfalls of risk assessments. cyberdb.co/6-common-pitfalls-of-information-security-risk-assessments/

[18] **CertificeringsAdvies** -- NIS2 checklist stappenplan, risicoanalyse frequentie. certificeringsadvies.nl/nis2-checklist-stappenplan-voor-de-nieuwe-cyberbeveiligingswet/

[19] **Digitale Overheid** -- Cyberbeveiligingswet: wie valt eronder, sectoren. digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[20]

Kynexis -- NIS2 boetes en handhaving, bestuurdersaansprakelijkheid. kynexis.nl/nis2-boetes-cyberbeveiligingswet-uitgelegd/

[21] **Banken.nl** -- 2026 wordt het jaar van geindustrialiseerde cybercriminaliteit en AI-agents. banken.nl/nieuws/26681/2026-wordt-het-jaar-van-geindustrialiseerde-cybercriminaliteit-en-ai-agents/