Auditdienst Rijk
Ministerie van Financiën

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

N Network

I Information

S Security

Cyberbeveiligingswet

Van Europese (NIS2-)richtlijn naar nationale wetgeving

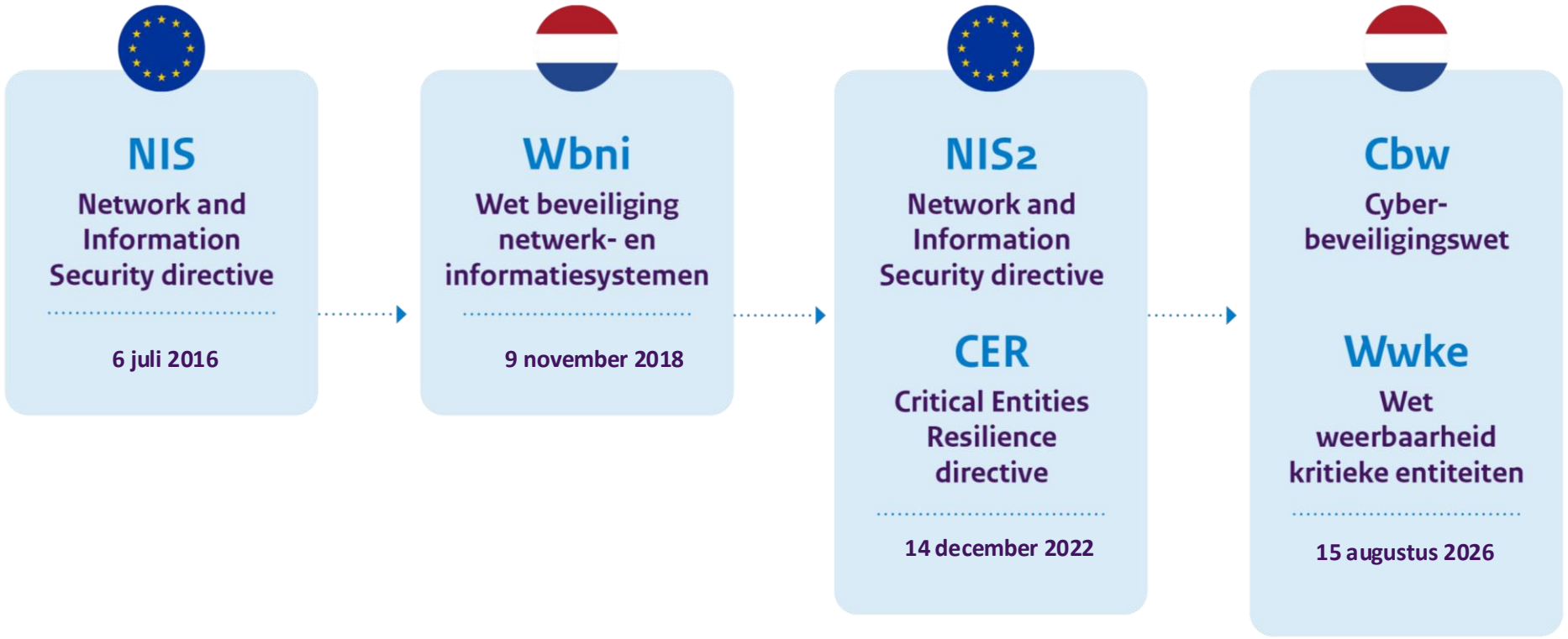
Melissa Taal

17 september 2026

Inhoud

I. Het wetgevingstraject
II. Weren producten en diensten van leveranciers
III. NIS2-simplificatie

Deel I – Het wetgevingstraject



Het wetgevingstraject

- **Voorbereiding**
- Interdepartementale werkgroep en stuurgroep
- Omzetting van bepalingen uit NIS2-richtlijn naar nationale wetgeving

- **Consultatie**
- Formele consultatie en internetconsultatie
- Verwerken consultatiereacties

- **Raad van State**
- Advies
- Nader rapport

Het wetgevingstraject

› **Tweede Kamer**

- Verslag
- Nota naar aanleiding van het verslag
- Wetgevingsoverleg 23 maart 2026

› **Eerste Kamer**

- Verslag
- Nota naar aanleiding van het verslag
- Stemming 7 juli 2026

Deel II – Weren producten en diensten van leveranciers

- Tijdens het wetgevingsoverleg amendement ingediend om deze bevoegdheid van de amvb over te hevelen naar de Cyberbeveiligingswet zelf

- **Waarom is deze bevoegdheid nodig?**

- Kwaadwillenden kunnen d.m.v. hun positie in de toeleveringsketen via entiteiten hun doelstellingen proberen te behalen
- Omdat dit de belangen van Nederland kan schade, is deze bevoegdheid opgenomen ter bescherming van de nationale veiligheid

- Een laatste redmiddel en alleen ingezet om nationale veiligheidsrisico's te beheersen

Weren producten en diensten van leveranciers

- **Welke risico's voor de nationale veiligheid kunnen een aanleiding zijn?**
- Sabotage
- Spionage
- Beïnvloeding door statelijke actoren of andere derden van netwerk- en informatiesystemen van een entiteit
- Ransomware-aanvallen die bijvoorbeeld de continuïteit van (vitale) processen verstoren of vertrouwelijke informatie doen weglekken

Weren producten en diensten van leveranciers

- **Weren van producten en diensten van leveranciers in de praktijk**
- De vakminister moet zich houden aan de kaders uit het artikel. Zo moet er sprake zijn van noodzakelijkheid én nationale veiligheidsrisico's
- Het opleggen gebeurt op individuele basis, dus per entiteit
- Er wordt risicogebaseerd bepaald welke product of welke dienst in welk proces van die entiteit geweerd wordt, dus maatwerk
- Inachtneming van de continuïteit van de dienstverlening
- Er staat bezwaar bij de vakminister en beroep bij de bestuursrechter open

III NIS2-simplificatie

- 20 januari 2026 een voorstel gepubliceerd tot simplificatie van de NIS2-richtlijn
- Onderhandelingen moeten nog beginnen
- Nederland zal de amendementen tegen die tijd opnemen in de Cyberbeveiligingswet

- **Belangrijkste onderdelen van het voorstel:**
- Het toepassingsbereik wordt uitgebreid en verduidelijkt
- De mogelijkheid om middels certificering aan te tonen dat je voldoet aan de zorgplicht
- Het kunnen inzetten van ENISA in geval van samenwerking tussen de bevoegde autoriteiten binnen de EU

Vragen?

N  Network

I  Information

S  Security

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Het toezicht op de wet in de praktijk

Toelichting toezicht Cbw

17 september2026

Rob Augustinus en Wietze Geertsma (inspecteur Digitale Weerbaarheid)

WOENSDAG 3 JUNI 2026 | PAGINA 7 NEDERLAND & TECH

Odido getroffen door cyberaanval, miljoenen klantgegevens gelekt

Telecombedrijf bevestigt dat persoonsgegevens van miljoenen klantaccounts zijn buitgemaakt na een cyberaanval.

Toch patiëntgegevens buitgemaakt bij hack op ChipSoft

Nieuwe informatie wijst uit dat bij de ransomwareaanval ook medische patiëntgegevens zijn buitgemaakt.

MAANDAG 11 MEI 2026 | BINNENLAND | 5

NNELAND • REGIONAAL

GEMEENTE HOF VAN TWENTE MOET MILJOENENSCHADE HACK ECHT ZELF BETALEN

Agenda

- Wat weten jullie al?
- Wat is de RDI?
- Wat is toezicht?
- Wat gaat de RDI doen?
- Afsluiting en vragen

Wat weten jullie al?

Quiz

Wat betekent de afkorting RDI?

A. *Rijksdienst Digitale Inspecties*
B. *Rijksdienst Digitale Infrastructuur*
✓ C. *Rijksinspectie Digitale Infrastructuur*
D. *Dutch Authority for Digital Infrastructure*

Wanneer mag een toezichthouder bij een belangrijke entiteit onderzoeken of deze zich aan de meldplicht of zorgplicht heeft gehouden?

A. *Periodiek*
✓ B. *Bij signalen van niet-naleving*
C. *Altijd*
D. *Na een incident*

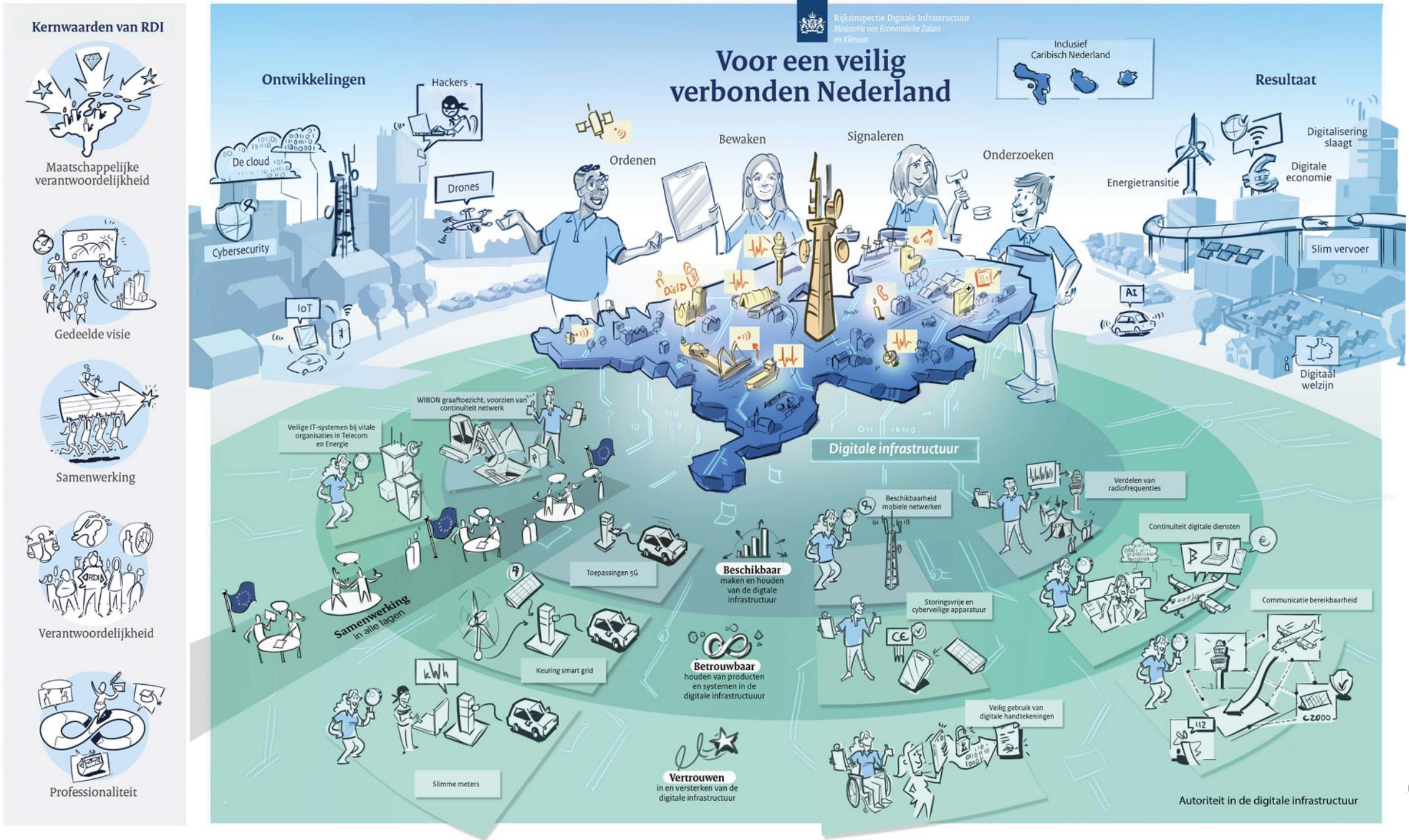
Bij een clouddienstverlener worden de beslissingen voor het beheer van cyberbeveiligingsrisico's genomen in Duitsland, zitten de meeste werknemers in Nederland en het SOC bevindt zich in Frankrijk. Waar jurisdictie?

A. *Frankrijk*
✓ B. *Duitsland*
C. *Meerdere landen*
D. *Nederland*

Wat is de RDI?

Rijksinspectie Digitale Infrastructuur

De RDI staat voor een veilig verbonden Nederland


Kernwaarden van RDI
Maatschappelijke verantwoordelijkheid
Gedeelde visie
Samenwerking
Verantwoordelijkheid
Professionaliteit
Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat
Voor een veilig verbonden Nederland
Inclusief Caribisch Nederland
Ontwikkelingen
Hackers
De cloud
Cybersecurity
Drones
IoT
Ordenen
Bewaken
Signaleren
Onderzoeken
Resultaat
Digitalisering slaagt
Digitale economie
Energietransitie
Slim vervoer
AI
Digitaal welzijn
Digitale infrastructuur
WIBON graaftoezicht, voorzien van continuïteit netwerk
Veilige IT-systemen bij vitale organisaties in Telecom en Energie
Samenwerking in alle lagen
Toepassingen 5G
Keuring smart grid
Slimme meters
Beschikbaar maken en houden van de digtale infrastructuur
Betrouwbaar houden van producten en systemen in de digitale infrastructuuur
Vertrouwen in en versterken van de digitale infrastructuur
Beschikbaarheid mobiele netwerken
Storingsvrije en cyberveilige apparatuur
Verdelen van radiofrequenties
Continuïteit digitale diensten
Communicatie bereikbaarheid
Veilig gebruik van digitale handtekeningen
Autoriteit in de digitale infrastructuur

Uitvoering en toezicht

- Cyberbeveiligingswet (Cbw)
- Wet weerbaarheid kritieke entiteiten (Wwke)
- Telecommunicatiewet
- eIDAS
- Cyber Security Act (CSA)
- Cyber Resilience Act (CRA)
- Radio Equipment Directive (RED)
- EMC-richtlijn (Electro Magnetic Compatility)
- LVD-richtlijn (Low Voltage Directive)
- Wet informatie-uitwisseling bovengrondse en ondergrondse netten en netwerken (WIBON)
- Metrologiewet (voorheen IJkwet)
- Waarborgwet
- Wet Ruimtevaartactiviteiten
- Wet Digitale Overheid

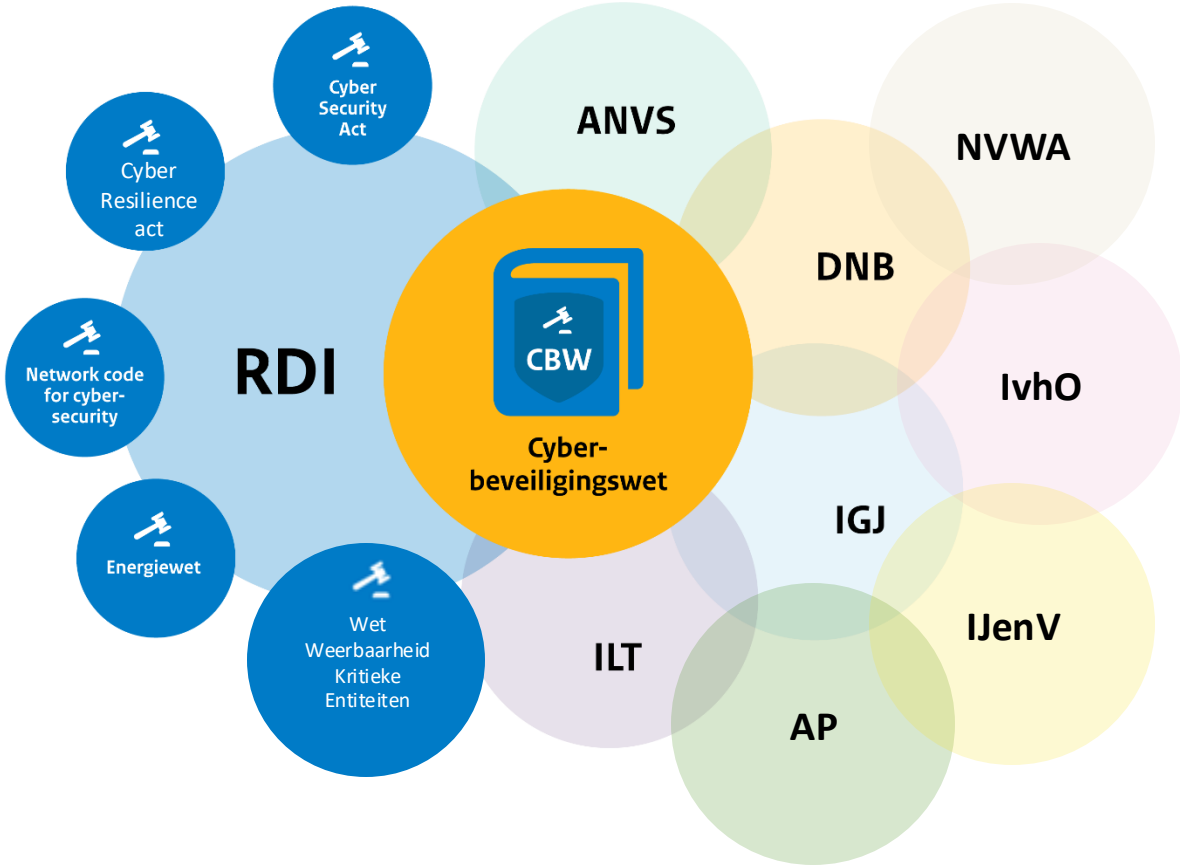
Cyberbeveiligingswet

- NIS2 in NL in Cbw geïmplementeerd
- Nadere uitwerking in:
  - Cyberbeveiligings**besluit** en
  - Ministeriële **regelingen**
  - **EU uitvoeringsverordening (2024/2690)**

  Opdrachtgevers voor RDI
  - **EZK** (o.a. digitale infrastructuur, beheer ICT diensten, ruimtevaart, vervaardiging, etc)
  - **KGG** (energie)
  - **BZK** (overheid)
- Inwerkingtreding: **15 augustus 2026**

Meer (nieuwe) wetgeving rondom (digitale) weerbaarheid

- Naast de Cbw ook andere wetten rondom digitale weerbaarheid
- Meerdere toezichthouders, met uiteenlopende opdrachten
- Entiteiten die in meerder sectoren vallen (dus meerdere toezichthouders)
- Samenwerking in STDW



(digitale) Weerbaarheid =

- bedreigingen kunnen weerstaan
- snel kunnen herstellen na verstoring of cyberaanval

Voorbeelden

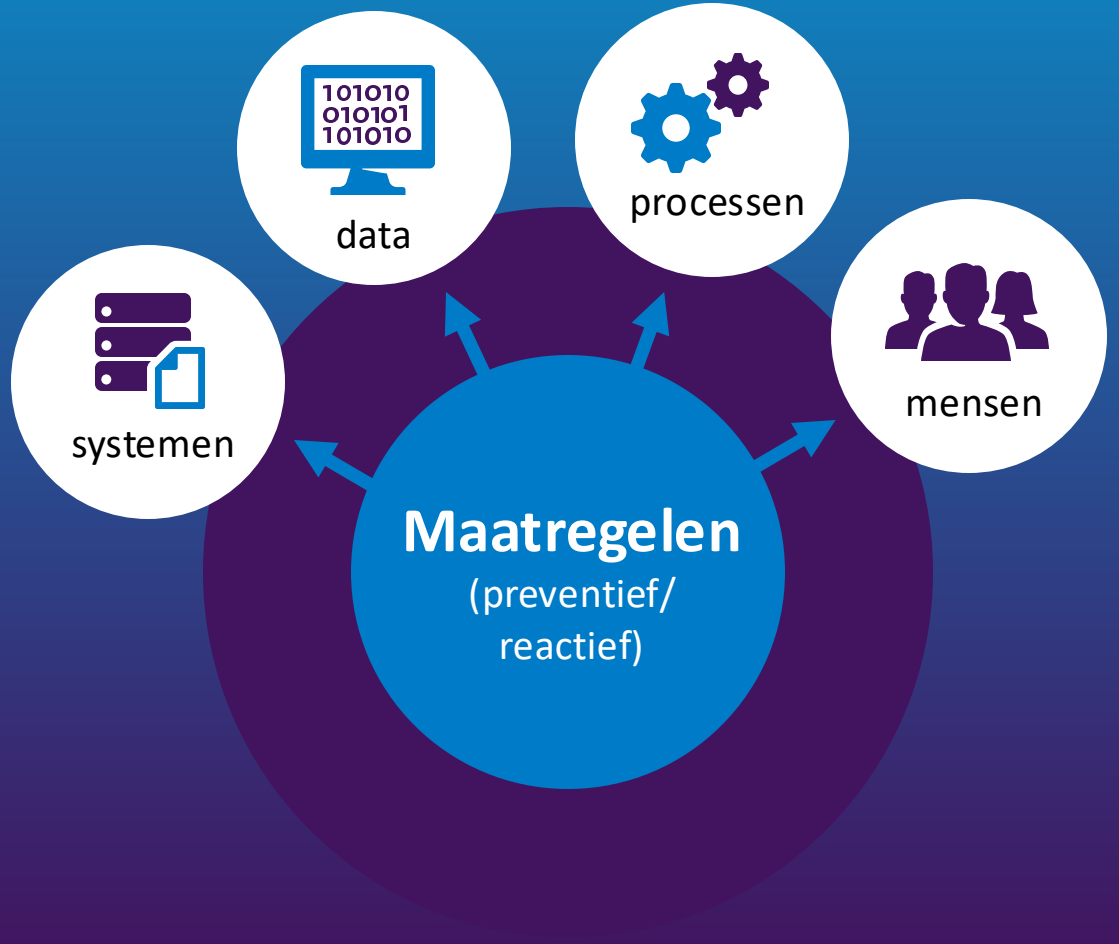
Dienstverlener die te maken krijgt met **gijzelsoftware**

Internetstoring bij een fabriek

Energiebedrijf dat wordt **gehackt**

(digitale) Weerbaarheid:

- vraagt om preventieve en reactieve maatregelen en voortdurend verbeteren
- verdient strategische aandacht binnen organisaties
- is cruciaal voor het vertrouwen van onze samenleving in digitalisering



We zetten de maatschappelijke opgave centraal en werken samen

Uitgangspunten voor onze werkwijze:

- **Digitale weerbaarheid** is een gezamenlijk doel
- We zetten onze **kennis en inzichten** in voor het publiek belang
- We stimuleren **samenwerking** tussen toezichthouders en andere overheden
- We werken risicogericht en informatie gestuurd

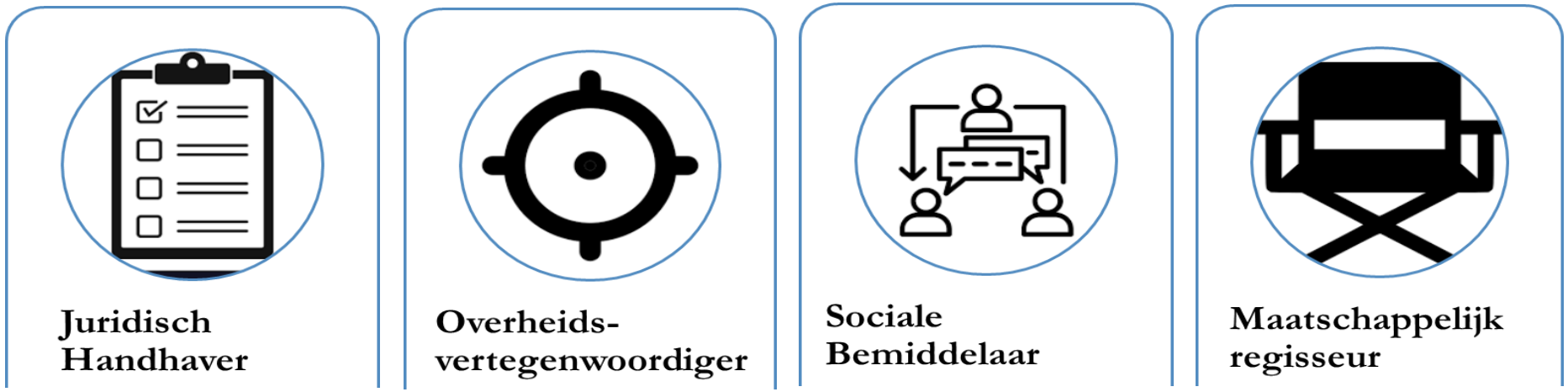
Wat is toezicht?

Wat is toezicht?

Toezicht is het verzamelen van de informatie over de vraag of een handeling of zaak voldoet aan de daaraan gestelde eisen, het zich daarna vormen van een oordeel daarover en het eventueel naar aanleiding daarvan interveniëren.

Onderbouwde en gerichte beïnvloeding van gedrag

Veranderende rol toezichthouder



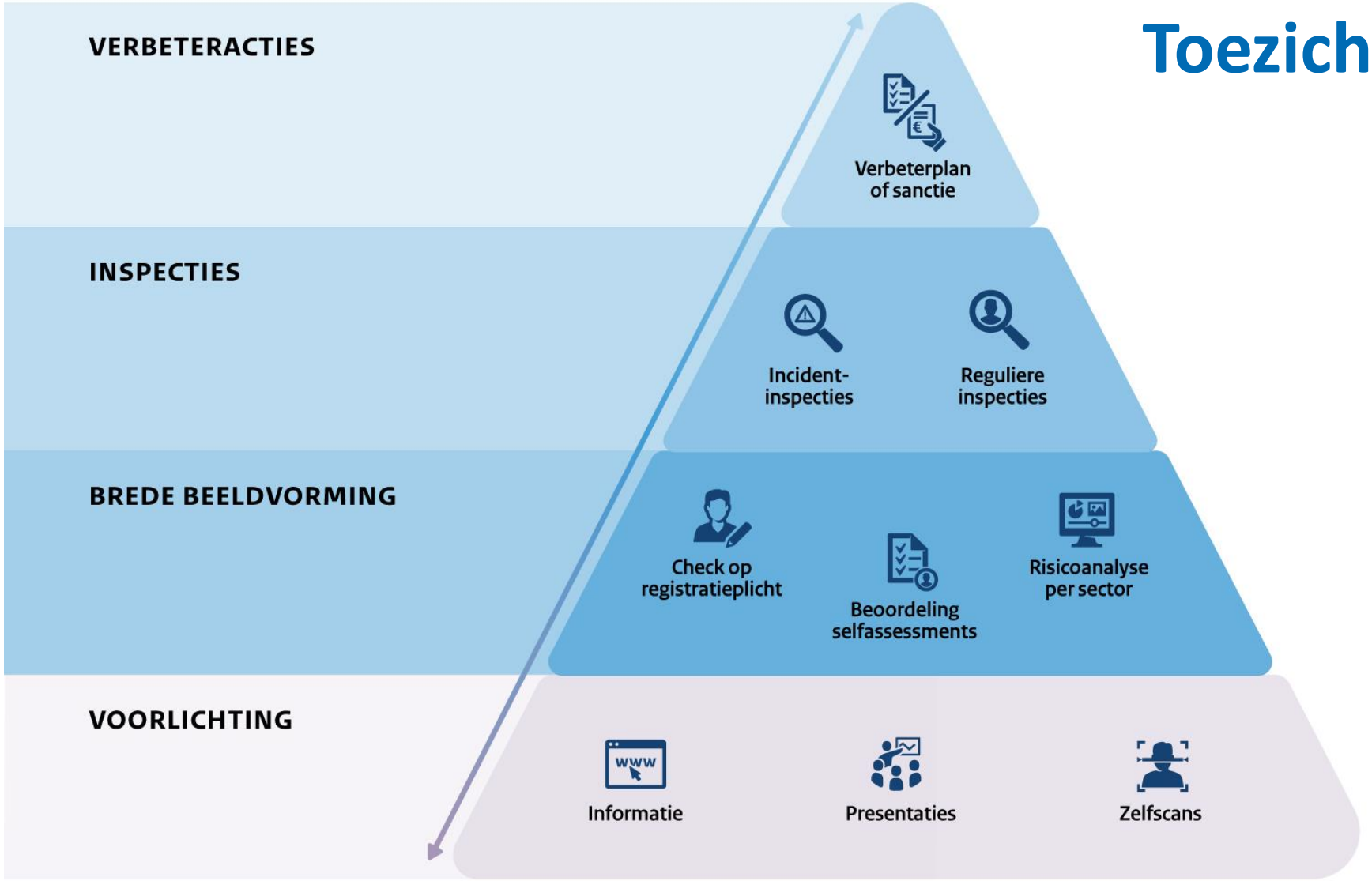
smal — breed

Rulebased
Nalevingsgericht
Legaliteit
Individueel

Riskbased
Probleemgericht
Legitimiteit
Stelsel/systeem

Naar Kasdorp

Toezichtsmodel



Wat gaat de toezichthouder dan doen?

Uit de Cyberbeveiligingswet volgen een aantal verplichtingen

Zorgplicht: uitvoering van passende technische en organisatorische maatregelen

Bestuur: goedkeuring van zorgplichtmaatregelen en trainingsverplichting voor bestuurders

Meldplicht: via centraal meldloket komt uw melding van ernstige ICT-incidenten bij CSIRT en toezichthouder

Registratieplicht: registratie in een entiteitenregister

Bij ons toezicht op digitale weerbaarheid werken we vanuit duidelijke uitgangspunten

We zetten het publieke belang centraal

We hebben een brede, onafhankelijke blik op het digitale stelsel

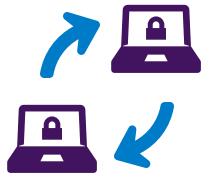
We zijn reflectief en risicogericht, en zien sancties als ultieme middel.

We werken samen met markt- en andere overheidsorganisaties

Organisaties moeten maatregelen nemen om aan de zorgplicht te voldoen

Voorbeelden

Uitvoering **risico-analyse**



Beveiliging van de **toeleveranciers-keten**

Borging **bedrijfs-continuïteit**

Beleid voor evaluatie van **effect maatregelen**

Verantwoordelijkheden van het bestuur

Onder de Cbw wordt cyberbeveiliging niet langer gezien als een technische kwestie, maar als een onderwerp voor de gehele organisatie.

Het bestuur is verantwoordelijk voor het beleid en de naleving van de wet.

- Daarom moeten bestuurders onder andere:
  - Aantoonbare kennis en vaardigheden hebben over risico's voor netwerk- en informatiesystemen, risicobeheersing en de impact van risico's op de organisatie;
  - Inzicht hebben in de risico’s en daarvoor passende maatregelen nemen om de digitale weerbaarheid van hun organisatie te waarborgen;
  - Regelmatig spreken met de eigen chief information security officer (CISO) over cyberbeveiliging.

De organisatie is zelf verantwoordelijk voor de invulling van maatregelen

Toezichthouders bepalen:

- **op welke manier** ze toezicht bij organisaties houden;
- **of passend invulling is gegeven** aan de verplichtingen uit de wet;
- **welke interventies** ze inzetten.

Hoe kan je met RDI toezicht te maken krijgen?

- We stimuleren en ondersteuning naleving met voorlichting en het bieden van handvatten
- We verzamelen informatie en maken en een inschatting de risico's
- We voeren op verschillende manieren inspecties uit en delen onze inzichten
- We stellen waar nodig verbeteracties voor en monitoren de opvolging

Werkwijze RDI voor Cbw

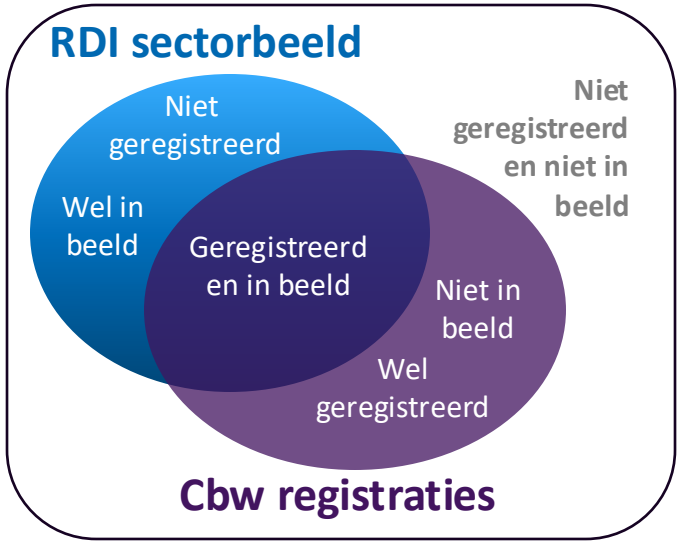
1. Registratie OTG via MijnNCSC, Na registratie MijnNCSC doorzetten naar RDI obv ingevulde Toezichthouder(s)

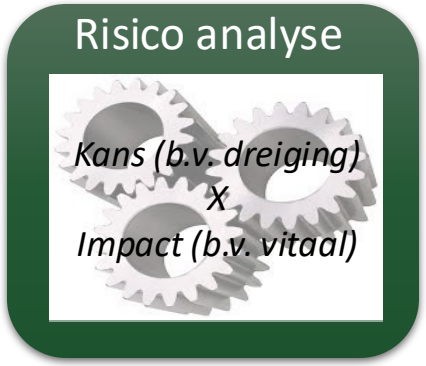
2. Kennismaking met geregistreerde entiteiten door brief en kennismakingsvragenlijst (entiteitbeeld en (sub)sectorbeeld)

3. Informatiegestuurd en risicogericht toezicht, breed naar smal:
   - Maatschappij/Politiek & Sectoren,
   - Eén Sector,
   - Eén of meerdere onder toezicht gestelde organisaties (OTG),
   - Eén OTG)

Informatiegestuurd en risicogericht toezicht

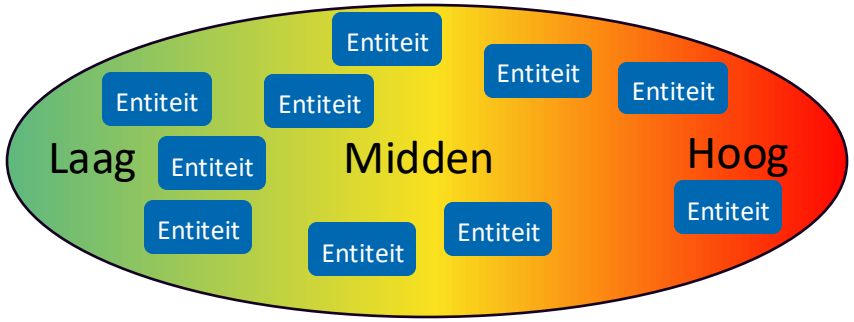
Sectorkennis
Openbare info
Overige bronnen





Indeling entiteiten binnen sector naar risicoprofiel

Soorten inspecties naar risicoprofiel:
- Administratief
- Standaard
- Incident



Thema’s Toezicht Cbw

Voor 2026 en 2027 onderdelen vanuit Cbw en maatschappelijk belang:

- Bestuursverantwoordelijkheid
- Registratieplicht
- Leveranciersketenmanagement
- Cloud
- OT
- AI
- Quantum/PQC
- …

Audit vs Toezicht

Aspect	Audit	Risicogestuurd toezicht
Doel	**Interne assurance:** Inzicht geven in de effectiviteit van eigen processen voor directie en stakeholders.	**Maatschappelijke preventie** publieke risico's beheersen.
Focus & Scope	**Rule-based & Organisatiegericht:** Toetsen tegen vaste interne normenkaders en audittrails.	**Principle-based & Keten/Governance:** Kijken naar volwassenheid, stuurlijnen en risicomanagement.
Risicoperspectief	**Geredeneerd vanuit organisatiedoelen** continuïteit en interne beheerskosten.	**Geredeneerd vanuit het publiek belang** Continuïteit van de dienstverlening voor de samenleving, privacy, milieu
Bewijsvoering	*"Design & Operating effectiveness"*: aannemelijkheid van effectiviteit via steekproeven.	*"Tell me, Show me, Prove me"* Patronen en systemische oorzaken die juridisch houdbaar zijn. Ook aantonen wanneer zaken er niet zijn.
Gevolgen & Interventie	Acties en aanbevelingen worden intern opgepakt; geen wettelijke sancties.	Vaststellen bevindingen & overtredingen, herstelmaatregelen of escalatie (verscherpt toezicht).

Hoe zal de toekomst eruit zien?

Alleen **samen** worden we **digitaal weerbaar**

Meer informatie?

RDI

↗ www.rdi.nl/cbw

worldstream

Onze NIS2 reis

17 September

Alan Lucas

Chief Information Security Officer @ WS & GHDC
Member of Sovereignty Committee @ CISPE
SOC Manager, Coach, Security Researcher @ DIVD

linkedin.com/in/alan-lucas

worldstream
greenhouse datacenters
DIVD Dutch Institute for Vulnerability Disclosure
CISPE.cloud

worldstream


greenhouse
53
53


worldstream

worldstream

DE PREMISSE

Compliance is de ondergrens

Compliance-denken

Doel geen bevindingen

Ritme jaarlijks, richting de audit

Scope de eigen perimeter

Bewijs documenten

statisch

Weerbaarheidsdenken

Doel adaptief vermogen

Ritme continu meten en bijsturen

Scope je gehele ecosysteem

Bewijs KPI's, oefeningen en trends

adaptief

worldstream

DE DRIE VERPLICHTINGEN

Waar zijn we begonnen?

01

Registratieplicht

Organisaties die onder de Cbw vallen melden zich aan in het nationale entiteitenregister bij de toezichthouder.

Eenmalig · Bij wijzigingen

02

Meldplicht

Significante incidenten zo snel mogelijk melden bij CSIRT en toezichthouder, met een vroege waarschuwing uiterlijk binnen 24 uur.

24u melding · 72u rapport · 1 mnd verslag

03

Zorgplicht

Risicoanalyse uitvoeren en passende, evenredige technische en organisatorische maatregelen treffen voor netwerk- en informatiesystemen.

Risicogebaseerd · 10 maatregelen (Art. 21)

BRON · NCSC.NL · CYBERBEVEILIGINGSWET (CBW) — IMPLEMENTATIE NIS2-RICHTLIJN (EU 2022/2555)

worldstream

UITGANGSPOSITIE & ANALYSE

Sterke basis, gerichte verbeteringen

GECERTIFICEERD

ISO 27001 · NEN 7510 · PCI-DSS
Information Security Management

GECERTIFICEERD

ISO 9001
Kwaliteitsmanagement & PDCA

ASSURANCE

ISAE 3402 & 3000
SOC 1 & SOC 2 Type II assurance

GEÏDENTIFICEERDE VERBETERINGEN 2025

Art. 21(3)	Leveranciers beter opnemen in risicoanalyse
Art. 22	Supply chain risicoanalyse op EU-niveau
Art. 23(1-2)	Incidentmelding aan CSIRT, toezichthouder én afnemers
Art. 27	Registratie in entiteitenregister
Art. 29	Cybersecurity informatie-uitwisseling
Art. 30	Vrijwillige melding van relevante informatie

worldstream

Herken de overlap

Als je al werkt met ISO 27001, PCI-DSS of financiële toezichteisen zoals DORA, dan heb je een voorsprong. De kunst is die overlap te herkennen en de delta gericht aan te pakken.

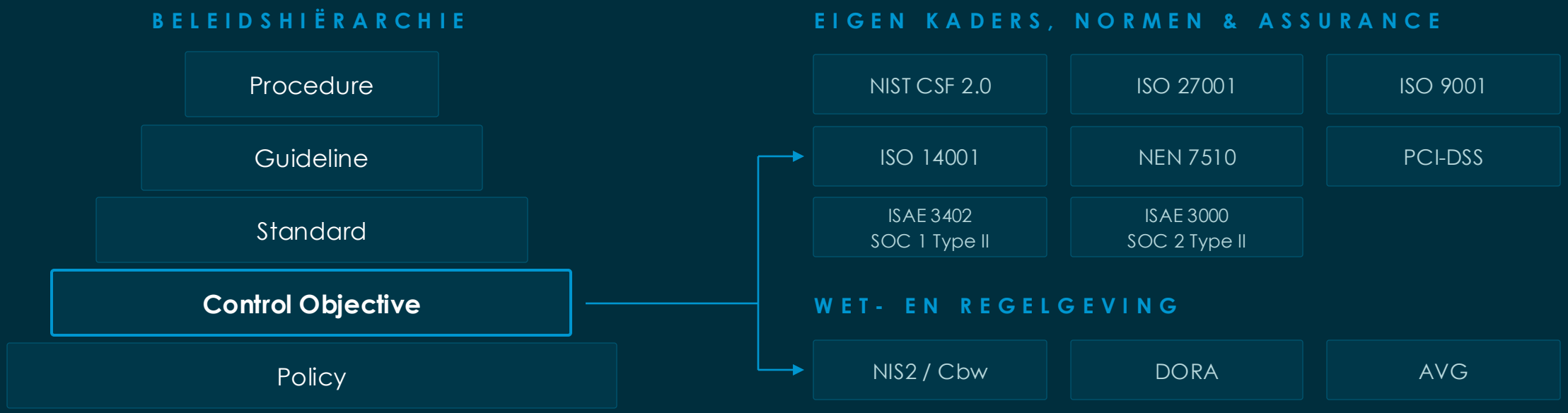
NIS2		DORA
24 uur	**Initiële melding**	4 uur
10 maatregelen (Art. 21)	**Risicoraamwerk**	Volledig ICT-risicokader
Effectiviteitsbeoordeling	**Penetratietesten**	TLPT (Threat-Led)

Breng ook je contractuele verplichtingen in kaart voordat je NIS2 gaat implementeren

worldstream

STRUCTUUR

Uniform managementsysteem (ISMS, QMS, EMS)



worldstream

GOVERNANCE

Het bestuur aan boord, en aan zet

01

2025 · Introductie

Wat NIS2 van ons vraagt en hoe wij het aanpakken, toegelicht in de boardroom.

02

Doorlopend · Rapportage

Periodieke herbeoordeling van risico's en maatregelen, met vaste rapportage aan het bestuur.

03

2026 · Crisisoefening

Het bestuur oefent zijn eigen rol. Besluiten en communiceren onder tijdsdruk.

EEN BESTUUR DAT GEOEFEND IS, BESLIST SNELLER

worldstream

MEETBAAR MAKEN · 1 VAN 2

KPIs

	Governance & risico	Asset management	Supply chain	CTEM
CONTROL STRENGTH / SECURITY LEVEL				
Control Maturity Level	NIST CSF 2.0 GOVERN	NIST CSF 2.0 IDENTIFY	NIST CSF 2.0 IDENTIFY	NIST CSF 2.0 PROTECT
Control Effectiveness / Health	% maatregelen op plandatum af Datum laatste BIA en scenarioset/RA % controls met geautomatiseerd bewijs	% applicaties met eigenaar % assets met classificatie # delta van de laatste inventarisatie	% compliant aan standaard % security clausules in contract # aanvullende beheersmaatregelen	% kritieke bevindingen binnen termijn # securityscore extern aanvalsoppervlak # securityscore interne assets
Control Coverage	% kritieke processen in de risicoanalyse	% applicaties / kritieke processen % assets in de CMDB	% leveranciers beoordeeld % leveranciers continu gemonitord	% assets gescand % internet-facing assets in AEV
Control Cost TCO per jaar	Per dienst	Per asset	Per leverancier	Per unit

worldstream

MEETBAAR MAKEN · 2 VAN 2

KPIs

	Identity & access	Human risk	Security operations	Continuïteit & crisis	Fysiek & omgeving
CONTROL STRENGTH / SECURITY LEVEL					
Control Maturity Level	NIST CSF 2.0 PROTECT	NIST CSF 2.0 PROTECT	NIST CSF 2.0 DETECT · RESPOND	NIST CSF 2.0 RECOVER	NIST CSF 2.0 PROTECT
Control Effectiveness / Health	% kritieke applicaties met ZTA # security posture score # uitzonderingen op IAM	% training afgerond # klik- en meldratio phishing	# tijd tot detectie en herstel (MTTD/MTTR) # doorlooptijd meldpad in tabletop exercities	% onafhankelijk getoetste hersteltests # RTO en RPO tegen eigen objectives % BCP's en DR's geoefend in de periode	% toegangsrechten tijdig herzien % facilitaire tests volgens schema
Control Coverage	% applicaties beheerd via IdP/IAM/PAM/PIM	% medewerkers en contractors % eindgebruikers in phishing	% assets onder monitoring % kritieke logbronnen ingested	% kritieke processen met getest BCP % kritieke data in backupscope	% kritieke systemen gemonitord
Control Cost TCO per jaar	Per identiteit	Per gebruiker	Per unit	Per dienst	Per locatie

worldstream

CONTINUE VERBETEREN

Wat wij concreet hebben gedaan

Supply chain versterkt

Leveranciersbeoordelingen uitgebreid met cybersecurity-criteria, exposure management (CTEM) en beheersing.

Art. 21(3) · Art. 22

Incident response aangescherpt

Communicatie en ketenverantwoordelijkheid centraal, informatiestromen naar toezichthouder, afnemers en ketenpartners.

Art. 23(1) · Art. 23(2)

Board

Ons bestuur begreep security al. Art. 20 gaf dat commitment een juridisch fundament, persoonlijke aansprakelijkheid formeel geborgd.

Art. 20 · Governance

Informatie-uitwisseling

Aansluiting bij sectorale informatie-uitwisseling. Dreigingsinformatie delen en ontvangen als structureel onderdeel van onze security operations.

Art. 29 · Art. 30

Doorlopende cyclus

Alle maatregelen ingebed in het PDCA-managementsysteem. Doorlopende controls met periodieke MT reviews en incident-oefeningen.

PDCA · ISO 27001 · ISO 9001

worldstream

ECOSYSTEEM

Weerbaarheid in de Communities

Dutch Datacenter Association

Sectorkennis en een gezamenlijke lijn voor datacenters.

Dutch Cloud Community

Praktijkervaring van Nederlandse cloud- en hostingproviders.

CISPE

Europese cloudinfrastructuur, beleid en soevereiniteit.

NCSC

Nationaal CSIRT. Dreigingsinformatie en meldpunt.

Autoriteiten

Formele lijnen en communicatie.

worldstream

WAT HET ONS HEEFT OPGELEVERD

Hoe NIS2 ons sterker heeft gemaakt

Meer grip op supply chain risico

Uitgebreide toetsing van onze leveranciers op hun cybersecuritypraktijken met structurele borging.

Incident response die werkt onder druk

Incident response aangescherpt op communicatie en ketenverantwoordelijkheid, informatiestromen naar toezichthouder, afnemers en ketenpartners bij incidenten.

Van overtuiging naar formele aansprakelijkheid

Art. 20 maakt het bestuur persoonlijk aansprakelijk. Dat is een hefboom die je kunt inzetten.

Geen project, maar operatie

NIS2 is geen eenmalig project maar onderdeel van onze PDCA-cyclus. Continue verbetering, geen eenmalige exercitie.

worldstream

AFSLUITING

Volg NIS2 niet om compliant te zijn. Gebruik de norm als instrument om **digitaal weerbaar** te worden.

Weerbaar worden, niet afvinken

Risicobeheer, incident response en supply chain security zijn operationele spieren. Die moet je trainen, niet alleen documenteren.

De CISO krijgt hefboom

Art. 20 maakt het bestuur persoonlijk aansprakelijk. Dat is geen last, het is je argument voor budget, aandacht en prioriteit.

Samen sterker als ecosysteem

Eerst frictie, dan fundament. Als elke schakel in de keten aantoonbaar weerbaar wordt, staat Europa er digitaal sterker voor.

NIS2 is het instrument. Digitale weerbaarheid is het resultaat. Een sterker Europa is de uitkomst.

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Auditdienst Rijk
Ministerie van Financiën

Cbw (NIS2) Control Framework

Getting in control of the Cbw & Cbb

Sandeep Gangaram Panday
(NOREA / Brightlyn)

17 september 2026

NOREA

Auditdienst Rijk
Ministerie van Financiën

Studierapport Cbw (NIS2) Control Framework

Een praktisch framework bij de implementatie van de Cyberbeveiligingswet (NIS2-richtlijn), voor het versterken van de digitale operationele weerbaarheid.

Auteurs
L.M. Molewijk, ADR
S. Gangaram Panday, Brightlyn
E. Hummel, ADR
T. Meeuws, ADR

Auditdienst Rijk
Postbus 20201, 2500 EE Den Haag
Telefoon: 088 – 442 80 00
E-mail:

NOREA
Postbus 242, 2130 AE Hoofddorp
Telefoon: 088 – 496 03 60
E-mail:

Cbw (NIS2) Control Framework onderschreven door

Statement van het NCSC alle toezichthouders op de Cbw

"Het NCSC en de Cbw-toezichthouders hebben kennisgenomen van het kader ontwikkeld door ADR en NOREA, dat erop gericht is de sector een framework te bieden voor de praktische implementatie van de Cbw, Cbb en sectorspecifieke eisen. Hoewel NCSC en de Cbw-toezichthouders niet hebben bijgedragen aan de ontwikkeling ervan of een diepgaande beoordeling hebben uitgevoerd, zien ze de creatie van dergelijke kaders als een goede invulling op hun eerdere oproepen tot sectorbrede samenwerking. Deze samenwerking is cruciaal voor het verbeteren van de algehele cyberweerbaarheid van de sector en, waar gewenst, gezamenlijk ontwikkelen en bijwerken van standaarden die aan dit doel kunnen bijdragen. NCSC en de Cbw-toezichthouders benadrukken dat naleving van de toepasselijke wetten en voorschriften de verantwoordelijkheid blijft van elke organisatie. Het kader kan organisaties helpen hun aanpak te structureren en te versterken, maar het blijft altijd de verantwoordelijkheid van de organisatie zelf om te beoordelen of zij volledig voldoen aan de toepasselijke wet- en regelgeving."

Nota Minister J&V, 29 juni 2026

De wetgever verwijst zelf ons framework

De regering tracht door middel van heldere toelichting, handreiking en communicatie de implementatie van de Cbw, waaronder de daarin opgenomen zorgplicht, zo eenvoudig mogelijk te maken. Daar is vanuit het bedrijfsleven ook behoefte aan. Bij de beoordeling welke specifieke maatregelen in het kader van de zorgplicht uit de Cbw genomen moeten worden, kunnen entiteiten gebruik maken van bestaande normenkaders, zoals ISO27001. Vanuit de rijksoverheid zijn voorts diverse tools en kennisproducten opgesteld die kunnen helpen bij het voldoen aan de zorgplicht uit de Cbw. Hieronder volgt een overzicht daarvan:

- Op de website van het Nationaal Cyber Security Centrum zijn meerdere infosheets te vinden over de zorgplicht uit de Cbw. Hierin wordt stap voor stap uitgelegd wat een entiteit kan doen om invulling te geven aan die verplichting. Ook worden er met enige regelmaat Q&A's hierover op de website van het Nationaal Cyber Security Centrum geplaatst.
- De Rijksinspectie Digitale Infrastructuur heeft een quickscan ontwikkeld waarmee entiteiten aan de hand van 40 vragen kunnen beoordelen hoe het met hun cyberbeveiliging ervoor staat.[3]
- De Auditdienst Rijk (ADR) en NOREA, de beroepsorganisatie van IT-auditors in Nederland, hebben in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties een *NIS2 Control Framework* ontwikkeld. Dit is bedoeld als praktisch hulpmiddel voor organisaties en IT-auditors om inzicht te krijgen in onder andere hun aanpak voor het voldoen aan de zorgplicht uit de Cbw.

Bron: Nota van de Minister van Justitie en Veiligheid, 29 juni 2026

"De Auditdienst Rijk (ADR) en NOREA hebben in opdracht van het Ministerie van BZK een NIS2 Control Framework ontwikkeld. Dit is bedoeld als praktisch hulpmiddel voor organisaties en IT-auditors."

- Geen nieuw normenkader: bestaande kaders zoals ISO 27001 mogen worden hergebruikt.
- Het ADR/NOREA-framework is de brug tussen de zorgplicht en concrete maatregelen.
- De RDI toetst met een quickscan van 40 vragen dezelfde taal, dezelfde onderwerpen.

Conceptversie juni 2025 vs. eindversie april 2026

Wat is nieuw?

- **Art. 21a – Weren van leveranciers (nieuw):** minister kan het gebruik van specifieke leveranciers of technologie verbieden en vervanging afdwingen. Gronden: nationale veiligheid, dreiging of banden met risicolanden.
- **Art. 21 lid 6 – Voorhangprocedure:** ontwerp-AMvB eerst 4 weken aan het Parlement voorleggen.

Wat is aangepast?

- **Bevoegde autoriteiten (art. 15):** duidelijkere toedeling per sector; decentrale overheden en waterschappen scherper gepositioneerd.
- **Meldplicht (art. 25):** explicietere koppeling met EU-uitvoeringshandelingen en nationale criteria.
- **Harmonisatie:** definities geactualiseerd; betere EU-aansluiting (o.a. eIDAS).

Wat is verwijderd?

- Geen wezenlijke verplichtingen geschrapt.
- De wet is vooral uitgebreid en aangescherpt.

Conclusie: de eindversie bevestigt grotendeels de conceptlijn, maar introduceert één fundamentele verschuiving — cybersecurity wordt niet alleen een risicomanagementvraagstuk, maar ook een instrument van nationale veiligheid.

Gepubliceerd 15 april 2026. Deze versie ligt ter accordering bij de Eerste Kamer en is pas na goedkeuring definitief.

Overview of EU Legislations in the Digital Sector

Network and Information Security Directive 2 (NIS2)

16/01/2023

= Applicable law

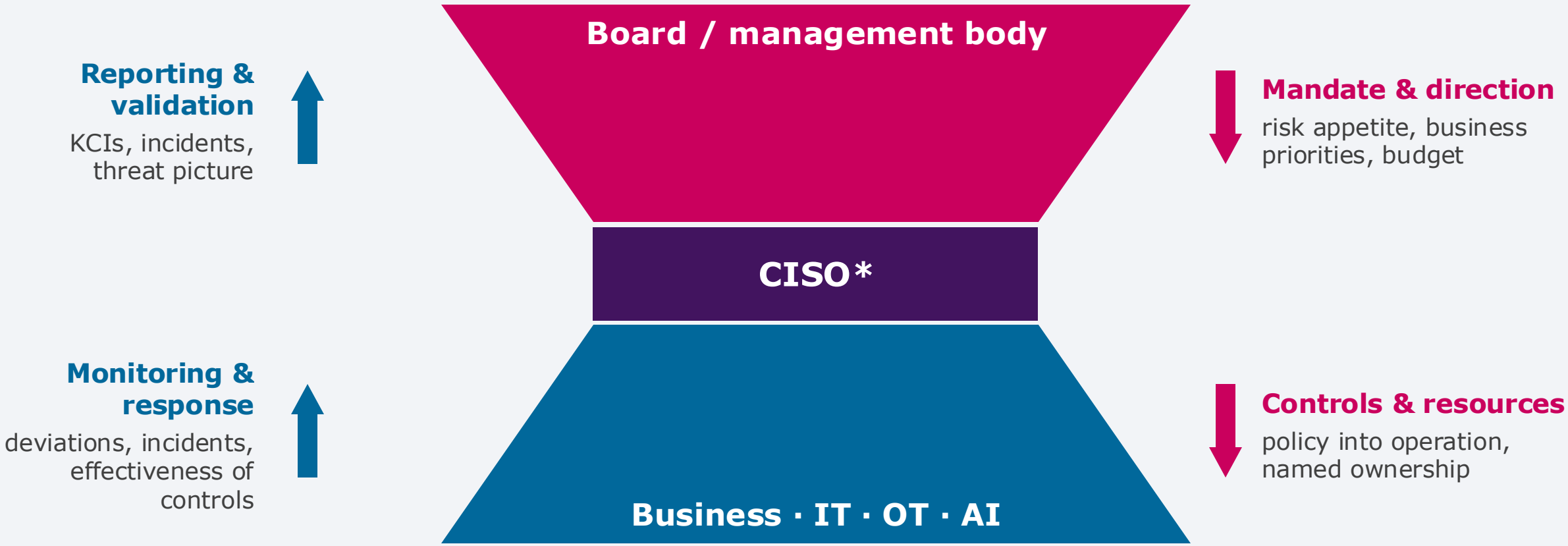
= In negotiation

= Planned initiative

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition & Single Market	Media	Finance
Digital Europe Programme Regulation (EU) 2021/694	Recovery and Resilience Facility Regulation (EU) 2021/241	Frequency Bands Directive (EEC) 1987/372	ePrivacy Directive (EC) 2002/58	Database Directive (EC) 1996/9	Regulation for a Cybersecurity Act (EU) 2019/881	Law Enforcement Directive (EU) 2016/680	Toys Regulation (EC) 2009/48, 2023/0290(COD)	Unfair Contract Terms Directive (UCTD) (EEC) 1993/13	EC Merger regulation (EC) 2004/139	Satellite and Cable Directive (EEC) 1993/83	Common VAT system (EC) 2006/112, 2022/0407(CNS), 2022/0409(CNS)
Horizon Europe Regulation (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation (EU) 2021/523	Radio Spectrum Decision (EC) 2002/676	European Statistics (EC) 2009/223	Community Design Directive (EC) 2002/6	Regulation to establish a European Cybersecurity Competence Centre (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment (EU) 2019/713	European Standardization Regulation (EU) 2012/1025	Price Indication Directive (EC) 1998/6	Technology Transfer Block Exemption (EC) 2014/316	Information Society Directive (EC) 2001/29	Administrative cooperation in the field of taxation (EU) 2011/16
Regulation on a pilot regime distributed ledger technology (EU) 2022/858	Connecting Europe Facility Regulation (EU) 2021/1153	Electromagnetic compatibility Directive (EMC) (EU) 2014/30	General Data Protection Regulation (GDPR) (EU) 2016/679	Enforcement Directive (IPR) (EC) 2004/48	NIS 2 Directive (EU) 2022/2555	Regulation on interoperability between EU information systems in the field of borders and visa (EU) 2019/817	Radio Equipment Directive (RED) (EU) 2014/53	E-commerce Directive (EC) 2000/31	Company Law Directive (EU) 2017/1132	Audio-visual Media Services Directive (AVMSD) (EU) 2010/13	Payment Service Directive 2 (PSD2) (EU) 2015/2366, 2023/0209(COD)
European Innovation Act	Regulation on High Performance Computing Joint Undertaking (EU) 2021/1173	Open Internet Access Regulation (EU) 2015/2120	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies (EU) 2018/1725	Protection of trade secrets (Directive) (EU) 2016/943	Cybersecurity Regulation (EU) 2023/2841	Regulation on terrorist content online (EU) 2021/784	eIDAS Regulation (European Digital Identity Framework) (EU) 2014/910	Unfair Commercial Practices Directive (UCPD) (EC) 2005/29	Screening of foreign direct investments Regulation (EU) 2019/452	Portability Regulation (EU) 2017/1128	Digital Operational Resilience Act (DORA Regulation) (EU) 2022/2554
	Regulation on Joint	European Electronic	Free flow of non-personal	Design Directive (EU) 2024/2823	Cyber Resilience Act (EU) 2024/2847	Temporary CSAM Regulation (EU) 2021/1232, 2022/0155(COD)	Regulation for a Single Digital Gateway (EU) 2018/1724	Directive on Consumer Rights (CRD) (EU) 2011/83	Market Surveillance Regulation (EU) 2019/1020	Satellite and Cable II Directive (EU) 2019/789	Crypto-assets Regulation (MiCA) (EU) 2023/1114
			ulsory licensing of 0129(COD)		Cyber Solidarity Act (Regulation) (EU) 2025/38	E-evidence Regulation (EU) 2023/1543	General Product Safety Regulation (EU) 2023/988	e-invoicing Directive (EU) 2014/55	P2B Regulation (EU) 2019/1150	Copyright Directive (EU) 2019/790	Anti-money laundering Regulation (AML) (EU) 2024/1624
					Information Security Regulation 2022/0084(COD)	Digitalisation of cross-border judicial cooperation (EU) 2023/2844	Machinery Regulation (EU) 2023/1230	Consumer Protection Cooperation Regulation (EU) 2017/2394	Single Market Programme (EU) 2021/690	European Media Freedom Act (EU) 2024/1083	Financial Data Access Regulation 2023/0205(COD)
					Digital package	Directive on combating violence against women (EU) 2024/1385	AI Act (Regulation) (EU) 2024/1689	Geo-Blocking Regulation (EU) 2018/302	Vertical Block Exemption Regulation (VBER) (EU) 2022/720		Payment Services Regulation 2023/0210(COD)
						Directive for combating sexual abuse and child sexual abuse material 2024/0035(COD)	Eco-design Regulation (EU) 2024/1781	Digital content Directive (EU) 2019/770	Digital Market Act (DMA Regulation) (EU) 2022/1925		Digital Euro 2023/0212(COD)
	Net Zero Industry Act (EU) 2024/1735	Digital Networks Act	collection for short-term rental (EU) 2024/1028			EU Digital Travel application, 2024/0670(COD)	Product Liability Directive (PLD) (EU) 2024/2853	Digital Contracts for Goods Directive (EU) 2019/771	Regulation on distortive foreign subsidies (EU) 2022/2560		Regulation on combating late payment 2023/0323(COD)
	EU Space Act	EU Cloud and AI Development Act	European Health Data Space (Regulation) (EU) 2025/327					Digital Services Act (DSA Regulation) (EU) 2022/2065	Horizontal Block Exemption Regulations (HBER) (EU) 2023/1066, (EU) 2023/1067		
	Quantum Act		Harmonization of GDPR enforcement procedures 2023/0202(COD)					Political Advertising Regulation (EU) 2024/900	Internal Market Emergency and Resilience Act (EU) 2024/2747		
	European Biotech Act		GreenData4all					Right to repair Directive (EU) 2024/1799	Platform Work Directive (PWD) (EU) 2024/2831		
	Advanced Materials Act		European Data Union Strategy					Digital Fairness Act	28th regime		
	Circular Economy Act								Revision of directives on Public Procurement		

Source : https://cdn.ceps.eu/wp-content/uploads/2025/07/CEPS-Zenner-Dataset-July-2025-1.pdf

Cyber governance is an hourglass, not a pyramid



Internal audit and risk report to the board independently

*or equivalent officer · adapted from: Guide to Cyber Security for Directors and Business Owners (CSR, September 2025), p. 17

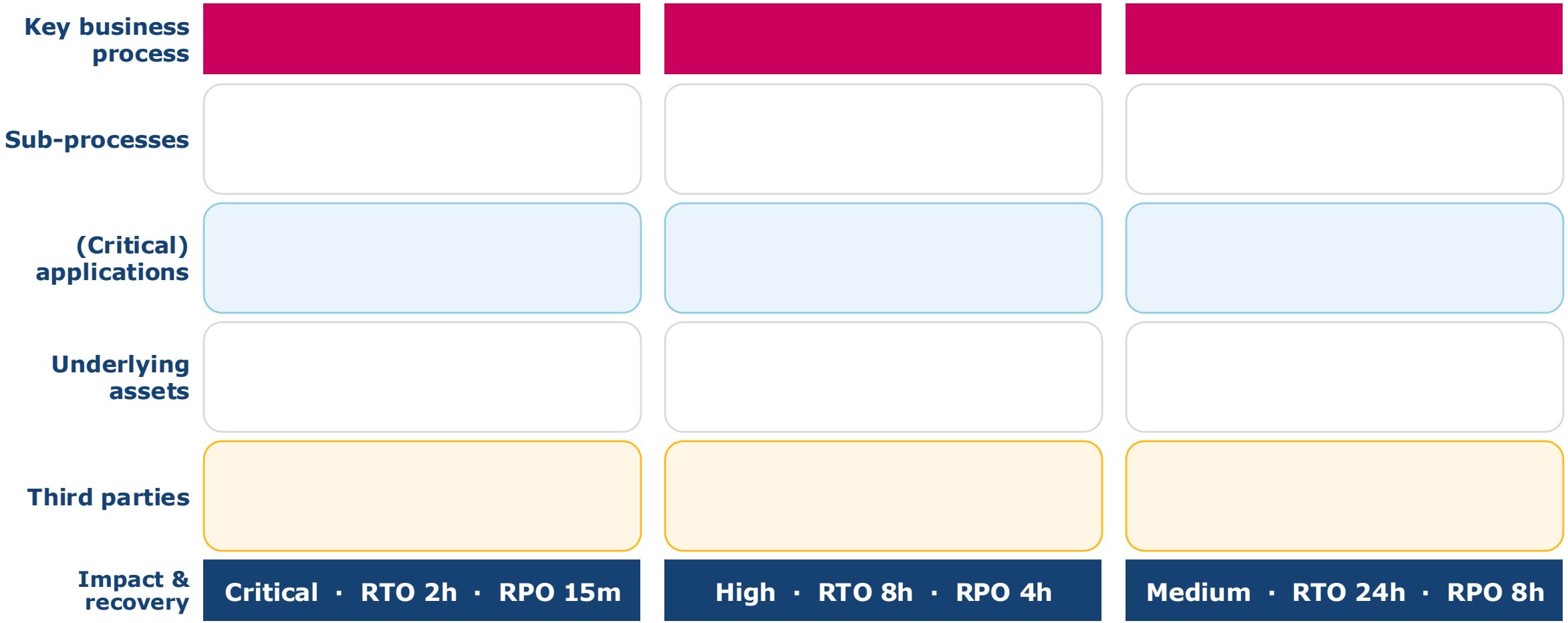
Recommended approach

STEP 1 OF 4

Asset inventory

What do we have and what does the business actually depend on?

From business process to underlying IT



Initial results from asset inventory

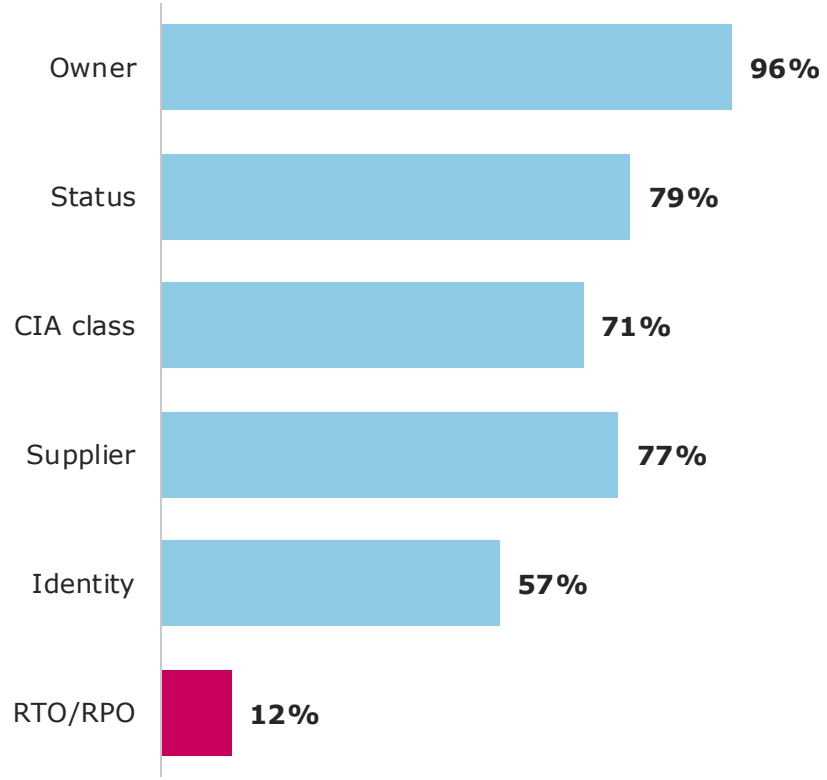
Question	Example results	Example remediation actions
1 **Which applications support a critical process?**	Usually 15–25% of the estate. In our example: 12 of 118 applications.	Set the strongest control baseline here first. Everything else can wait a cycle.
2 **Which applications have no owner or a stale status?**	25 of 118 had no reliable status: unknown, unspecified or due for replacement.	No owner means no control. Assign an owner or decommission.
3 **Which applications sit outside central identity?**	48 of 118 are not behind the central IdP, 17 more are unknown.	MFA and joiner/mover/leaver cannot be enforced. Onboard, or log a dated exception.
4 **Where is supplier concentration highest?**	Four vendors supply 60% of the landscape; 35 vendors supply one application each.	Deep assurance on the top four, light-touch questionnaire for others.
5 **Which third parties can halt a critical process?**	Two suppliers sit inside the payment chain with no tested fallback.	Security clauses, exit plan and an annual failover test in the contract.
6 **Which assets are reachable from the internet?**	Front-ends, gateways and remote access: typically, under 10% of all assets.	First in line for hardening, patch SLA and external vulnerability scanning.

Nine important fields per application

MINIMUM RECORD · EXAMPLE: PAYMENT HUB

Application name	Payment hub
Business owner	Head of Operations (named person)
Status	Active — in production
Supports process	Disburse & collect funds (critical)
CIA classification	C high · I high · A critical
RTO / RPO	2 hours / 15 minutes
Identity method	Central IdP + MFA enforced
Supplier & model	Vendor X · SaaS · SOC 2 Type II
Hosting & data location	EU region · managed hosting partner

FIELD COMPLETENESS ACROSS 100 APPS



STEP 2 OF 4

Risk assessment

What can go wrong, how badly would it hurt and how likely is it today?

Risk assessment in 4 steps

1 Business impact

GOAL

Know what breaks, and how fast it starts to hurt.

OUTPUT

Add CIA rating to every (sub)process taking full chain into account

2 Threat scenarios

GOAL

Agree what can plausibly go wrong.

OUTPUT

8–10 standard scenarios, mapped to the processes they threaten.

3 Risk scoring

GOAL

Judge how likely it is, given the controls you already have.

OUTPUT

A scored risk per scenario.

4 Treatment

GOAL

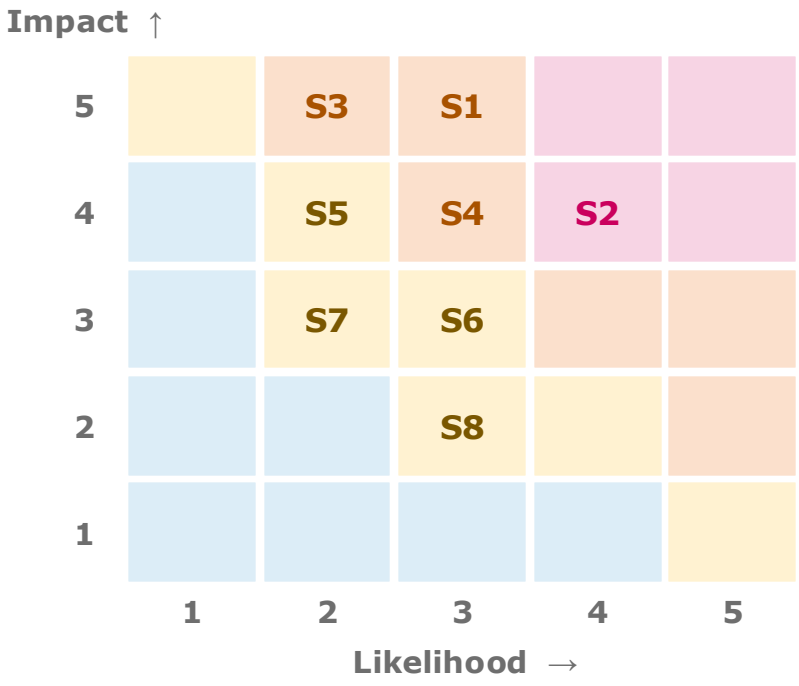
Decide: accept, mitigate, transfer or avoid.

OUTPUT

A dated decision, with an owner and a budget behind it.

One scenario set for the whole organisation

	Scenario	Imp.	Likel.	Risk
S1	Ransomware encrypts core systems	5	3	High
S2	Internet-facing vulnerability exploited	4	4	Critical
S3	Privileged account compromised	5	2	High
S4	Critical supplier outage beyond RTO	4	3	High
S5	Client data leak via misconfiguration	4	2	Medium
S6	DDoS against the public front-end	3	3	Medium
S7	Insider misuse of standing access	3	2	Medium
S8	Loss of key personnel and knowledge	2	3	Medium



STEP 3 OF 4

Gap assessment

Which controls are missing, and can we prove the ones we already have?

17 domains, grouped into 7 recognizable buckets

Governance & risk — 3

1 Network & information systems policy

2 Risk management policy

3 Evaluation & effectiveness review

OWNER: CISO / risk

Protect — 4

7 Acquiring, developing & maintaining

9 Cryptography

11 Logical & physical access security

12 Asset management

OWNER: IT security

Detect & respond — 2

4 Incident handling

13 Alerts, advice & information sharing

OWNER: SOC / IT ops

Resilience — 1

5 Business continuity & crisis management

OWNER: Business continuity

Supply chain — 1

6 Supply-chain security

OWNER: Procurement

People — 3

8 Cyber hygiene & training

10 Personnel security

14 Board training & certification

OWNER: HR / CISO

Regulatory reporting — 3

15 Reporting obligations

16 Early-warning requirements

17 Further incident notification

OWNER: Compliance

Maturity model

LEVEL 1 Ad hoc

No formal control. It happens when someone remembers.

PROOF REQUIRED

Nothing to show.

LEVEL 2 Partial

Documented or done in places, inconsistently applied.

PROOF REQUIRED

A policy, or one team doing it well.

LEVEL 3 Proven

A formal process, applied and provable across scope.

PROOF REQUIRED

Procedure, named owner, records of it running.

LEVEL 4 Managed

Measured, periodically tested and actively steered.

PROOF REQUIRED

Test plan, results, management review minutes.

LEVEL 5 Optimised

Automated or fully integrated, improving on its own.

PROOF REQUIRED

Metrics and evidence of improvement over time.

Left of here you cannot evidence compliance

Practical threshold · Level 3 minimum, Level 4 where it is critical

2 → 3

A written procedure, a named owner, and proof that it was actually followed.

3 → 4

A test plan, recorded results, and a periodic management review of both.

4 → 5

Metrics, automation, and demonstrable improvement over consecutive periods.

STEP 4 OF 4

Roadmap

What do we do first, who owns it, and what exactly is the board funding?

From gaps to a roadmap

Prioritise: Anything that reduces a Critical scenario goes to Now.

NOW 0–3 months

Enforce MFA on the 12 applications behind critical processes

OWNER: IT security

Give every application an owner and a current status

OWNER: CISO

Close the two internet-facing vulnerabilities on the payment front-end

OWNER: IT operations

Rehearse the 24h / 72h incident notification path end to end

OWNER: Compliance

NEXT 3–9 months

Onboard remaining applications to central identity, or log dated exceptions

OWNER: IT security

Independently test access recertification and backup restore

OWNER: Internal audit

Security clauses and exit plans for the top four suppliers

OWNER: Procurement

Board training plus one tabletop crisis exercise

OWNER: CISO / HR

LATER 9–18 months

Automate evidence collection for the recurring controls

OWNER: IT security

Continuous monitoring for the long-tail suppliers

OWNER: Procurement

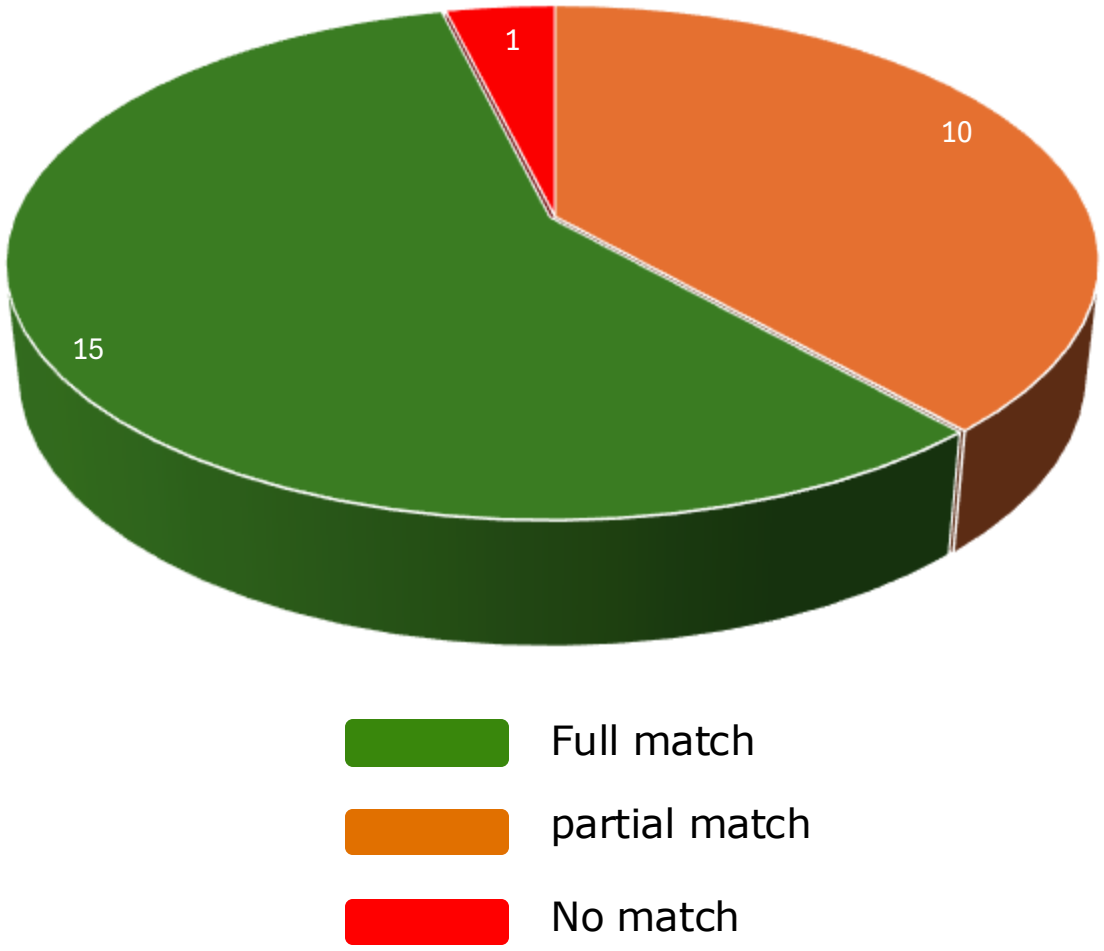
Lift domains carrying critical processes from Level 3 to Level 4

OWNER: Risk

Annual re-run of the BIA and the scenario set

OWNER: Risk

ISO27001 mapping



Partial match:

- Logging specific incident information
- Specific BCP items
- Crisis management plan
- Periodic assessment of supplier
- Specific software lifecycle controls
- Training of boardroom members < 2 years
- Reporting of significant incidents

No match:

- Significant incident reporting timelines

Question or suggestions?

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Auditdienst Rijk
Ministerie van Financiën

Edwin Hummel
e.hummel@minfin.nl

Marleen Molewijk
l.m.molewijk@minfin.nl

Sandeep Panday
sandeep@brightlyn.nl

Or download at:

www.norea.nl/regulatory

www.auditdienstrijk.nl/kennis-delen/onze-tools/cbw-nis2-control-framework

PANELDISCUSSIE | *Cbw in de praktijk*

- Sandeep Gangaram Panday
- Melissa Taal
- Rob Augustinus
- Wietze Geertsma
- Alan Lucas

GEZELLIGE BORREL

DANK VOOR UW AANWEZIGHEID
EN EEN SUCCESVOL EVENT!