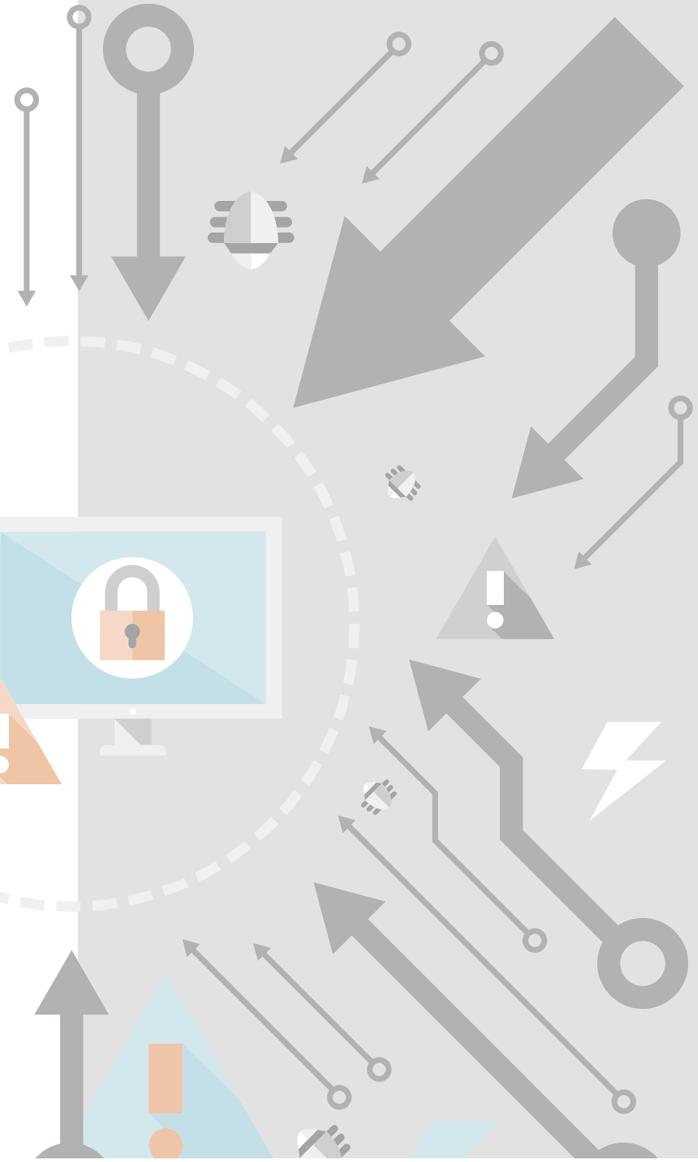
CSR Cyber Security Raad

HANDREIKING CYBERSECURITY VOOR BESTUURDERS EN BEDRIJFSEIGENAREN



INHOUDSOPGAVE

1. Doelgroep van deze handreiking **4**

2. Waarom is deze handreiking belangrijk voor u? **6**

3. Het doel is cyberveiligheid en weerbaarheid van uw organisatie **8**

4. Welke vragen moet u als bestuurder stellen? **10**

5. Prioriteit stellen om uw cyberrisico effectief te beperken **12**

6. Continu toezicht – governance **16**

7. Juridische aspecten van uw bestuursverantwoordelijkheid **20**

8. Verantwoordelijkheid voor cyberrisico's is niet beperkt tot uw eigen organisatie **22**

9. Externe rapportageverplichtingen **24**

10. Bestuurderstraining met impact **26**

11. Houd de vinger aan de pols en verbeter waar nodig **28**

12. De juiste toon aan de top - geef het goede voorbeeld **30**

13. Dankwoord **32**

14. Bijlagen **34**

Bijlage 1: Lijst van afkortingen en terminologie **34**
Bijlage 2: Niet-uitputtende lijst van cyberrisico's **35**
Bijlage 3: Checklist voor bestuurders **36**
Bijlage 4: Meer informatie over specifieke Nederlandse wettelijke voorschriften **37**
NIS2 – Cyberbeveiligingswet **37**
NIS2 Cyberbeveiligingswet – Verantwoordelijkheden bestuurders 37
NIS2 Cyberbeveiligingswet – Toeleveringsketen vereisten 38
NIS2 Cyberbeveiligingswet - Aansprakelijkheden bestuurders 38
NIS2 Cyberbeveiligingswet - Trainingsvereisten 40
Lees meer over DORA **40**
DORA - Verantwoordelijkheden bestuurders 41
DORA – Aansprakelijkheden bestuurders 41
Lees meer over CER **42**
Lees meer over CRA **42**

1. DOELGROEP VAN DEZE HANDREIKING

Deze handreiking is bedoeld voor zowel bestuurders en bedrijfseigenaren, als leden van raden van commissarissen of toezicht in **alle** organisaties. Dit is ongeacht hun omvang en of ze publiek of privaat zijn. De handreiking is ook bedoeld voor bestuurders en eigenaren van bedrijven die niet onder de nieuwe cyberwetgeving zoals NIS2 of DORA vallen. Hierna gebruiken we de term ‘bestuurders’, waarmee we doelen op zowel bestuurders en bedrijfseigenaren, als leden van raden van commissarissen of toezicht. De handreiking is geschreven vanuit een Nederlands perspectief en verwijst daarom naar de Nederlandse wetgeving. De aangebrachte inzichten zijn echter breed toepasbaar.

***Cyberdreiging** is meestal een externe factor en is gekoppeld aan tegenstanders (cybercriminelen, vijandige staten) die uw organisatie (of een toeleverancier) schade willen en kunnen berokkenen*

---

2. WAAROM IS DEZE HANDREIKING BELANGRIJK VOOR U?

Onze samenleving, economie en nationale veiligheid zijn sterk afhankelijk van informatie- en communicatietechnologie (ICT). Ook de aansturing van machines in de productielijn en de logistieke infrastructuur van bedrijven is steeds vaker aan het internet gekoppeld. We zijn kwetsbaar als er iets misgaat en veel organisaties zijn niet goed voorbereid op een “no-ICT” situatie. In tijden van geopolitieke onrust zijn bedrijven kwetsbaarder voor digitale verstoringen. Cyberbeveiliging is niet langer alleen een ICT-vraagstuk, maar een strategische prioriteit voor bestuurders.

Bestuurders hebben een algemene wettelijke plicht om hun taak behoorlijk te vervullen.[1] Daaronder valt het borgen dat hun organisatie beschikt over adequaat werkende risicobeheersings- en controlesystemen. Cyberbeveiligingsrisico’s staan steevast in de top drie risico’s voor elke organisatie. Het is daarom belangrijk dat bestuurders over voldoende cyberexpertise beschikken en dat cyberrisico’s worden ingebed in de reguliere risicobeheersings- en controlesystemen. Cyberbeveiligingsrisico’s zijn een **strategisch** risico. Niet kan worden volstaan met het delegeren van de verantwoordelijkheid aan de IT-afdeling of de functionaris voor informatiebeveiliging en het beperken tot het jaarlijks goedkeuren van budgetten.

De Europese wetgevers hebben in DORA[2] en NIS2[3] de verplichtingen voor bestuurders van financiële instellingen en kritieke infrastructuur nader uitgewerkt.[4] De impact van deze wettelijke bepalingen is verstrekkend. Zij vereisen dat organisaties adequate maatregelen treffen om cyberbeveiligingsrisico’s te beheersen, bepalen dat het de taak is van bestuurders om deze maatregelen goed te keuren, toezicht te houden op de uitvoering ervan en dat bestuurders daarvoor ook aansprakelijk kunnen worden gehouden. Ook stellen ze eisen aan de opleiding, kennis en expertise van bestuurders.

Deze vereisten zijn niet alleen relevant voor organisaties die rechtstreeks onder de nieuwe wetgeving vallen. Door de toenemende cyberdreiging geldt voor alle organisaties dat bestuurders hun verantwoordelijkheid moeten nemen. Kortom, het beheer van cyberrisico’s vormt een integraal onderdeel van uw taak als bestuurder. Deze handreiking heeft als doel u daarbij te helpen, waarbij voor kleinere bedrijven uiteraard een vertaalslag kan worden gemaakt naar de realiteit van een kleinere organisatie. Hierna bespreken we bijvoorbeeld de rol van een Chief Information Security Officer (CISO)[5]. Bij kleinere organisaties is het niet altijd haalbaar een CISO aan te stellen, en kunnen de taken bij andere werknemers worden belegd.

1 Art. 9(1) Boek 2 BW.

2 Digital Operational Resilience Act (DORA), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

3 Network and Information Security Directive (NIS2), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

4 Zie voor een actueel overzicht van alle Europese regelgeving die impact heeft op IT risk management en compliance, zoals cybersecurity en cyberweerbaarheid, https://www.norea.nl/nieuws/otc-en-norea-publiceren-nieuwe-editie-van-het-wetgevingsoverzicht

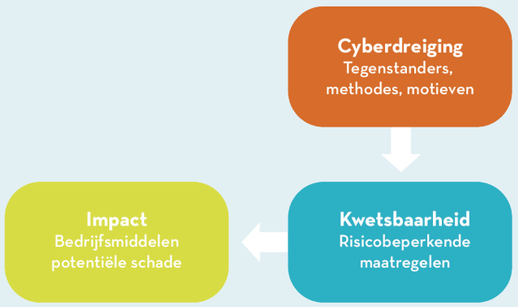
5 Chief information security officer - Wikipedia

3. HET DOEL IS CYBERVEILIGHEID EN WEERBAARHEID VAN UW ORGANISATIE

Naleving van regelgeving is belangrijk voor elke organisatie. Zonder naleving van wetgeving staat de *'license to operate'* van uw organisatie onder druk. Maar compliance is geen doel op zich, het is een middel om een doel te bereiken - namelijk het borgen van het succes en de continuïteit van de bedrijfsprocessen van uw organisatie en beveiliging van gegevens van klanten of burgers. Waar cyber- beveiligingsrisico's kritiek zijn voor het realiseren van de strategie, zou de **intrinsieke motivatie** om deze op bestuursniveau te adresseren voorop moeten staan. Uw organisatie kan niet functioneren als uw ICT niet goed functioneert en dat geldt ook voor uw toeleveringsketen.

De ICT van uw organisatie is in de meeste gevallen geen ondersteunende functie, maar een primair bedrijfsproces. Dit lijkt een open deur, maar moet toch worden vermeld. Bijvoorbeeld online bankieren is een primair bedrijfsproces en bestaat voornamelijk uit een ICT-platform. Als dit ICT-platform wordt beschadigd of verstoord, is het primaire proces niet meer uitvoerbaar. Dit geldt ook voor productiebedrijven waarbij bijv. machines op afstand worden aangestuurd en gemonitord. Het beheer van cyberrisico's en het verhogen van de cyberweerbaarheid (bijv. door goede back-up van uw gegevens en uitwijkvoorzieningen), moeten deel uitmaken van uw strategische doelstellingen en uw activiteiten als bestuurder.

Figuur 1: Cyberrisico als een combinatie van factoren



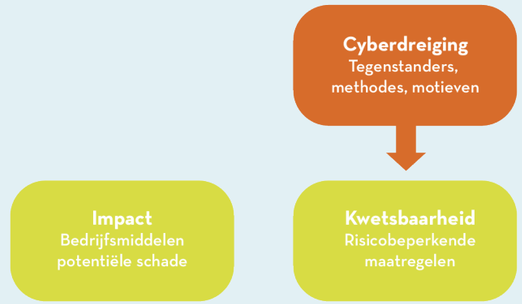
Cyberrisico´s zijn bedrijfsrisico's. Begrippen als risicobeperking, risicobereidheid en restrisico zijn niet nieuw. Risico is een combinatie van 'impact' en 'waarschijnlijkheid'. Cyberrisico's kunnen ontstaan door menselijke fouten (bijv. als de opties die software biedt niet goed zijn ingesteld) of kan het gevolg zijn van uitval van ICT in de toeleveringsketen. Anders dan de meeste bedrijfsrisico's wordt het cyberrisico echter voor een groot deel bepaald door **intentionele dreiging van externe actoren**. Voor cyberrisico's gebruiken we daarom een model met een derde factor, de cyberdreiging.

Impact is verbonden met uw bedrijfsmiddelen en de mogelijke impact op het functioneren van uw organisatie. Denk hierbij bijvoorbeeld aan een onderbreking van de dienstverlening, diefstal van intellectueel eigendom of geheime informatie, lekken of wijzigen van persoonsgegevens, schade aan personen en reputatie. Het betreft de mogelijke gevolgen van de drie factoren van ICT-beveiliging: het borgen van de **vertrouwelijkheid, integriteit** en **beschikbaarheid** van informatie.

Cyberdreiging is meestal een externe factor en is gekoppeld aan tegenstanders (cybercriminelen, vijandige staten) die uw organisatie (of een toeleverancier) schade willen en kunnen berokkenen.[6]

De laatste factor is **kwetsbaarheid**. Dit is de factor waarop u invloed kunt uitoefenen door risicobeperkende maatregelen toe te passen op uw ICT-systemen, in het vakjargon worden dit '*controls*' genoemd. ICT-systemen zijn servers, databases, operationele technologie (OT), netwerk- en cloud-infrastructuur... Voorbeelden van '*controls*' zijn het gebruik van *multi-factor authenticatie* (MFA) bij het aanmelden, het beheer van geprivilegieerde toegangsrechten en maatregelen voor de bedrijfscontinuïteit in het geval er iets misgaat (een betrouwbare back-up van bedrijfsgegevens en uitwijk).

Figuur 2: Vermindering van het risico door goed functionerende risicobeperkende maatregelen



Wanneer de risicobeperkende maatregelen goed zijn afgestemd op de cyberdreiging zou de impact op uw bedrijfsmiddelen binnen uw risicobereidheid moeten blijven.
Stel uzelf en uw medebestuurders allereerst de vragen: Hoeveel risico willen we lopen?

6 https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland

4. WELKE VRAGEN MOET U ALS BESTUURDER STELLEN?

Wat is onze **risicobereidheid**?[7] Hoeveel verstoring van onze organisatie is aanvaardbaar? Hoe schadelijk is het als we onze kennis of intellectueel eigendom door bedrijfsspionage verliezen aan een concurrent?[8] Hoe erg is het als we met een cyberincident voorpaginanieuws worden? Wat zijn de gevolgen van een lek van persoonsgegevens? Welk budget zijn we bereid te spenderen voor het afhandelen van cyberincidenten? Hoe gaan we om met cyberafpersing (*ransomware*)? In de bijlage vindt u een - niet-uitputtend - overzicht van risico's die mogelijk herkenbaar zijn voor uw organisatie.

Stel u ook de vraag hoe goed de veiligheidscultuur is in uw organisatie. Kunnen medewerkers hun zorgen kenbaar maken? Zijn de rollen en verantwoordelijkheden voor cyberrisicobeheersing goed toebedeeld?

Als bestuurder dient u vervolgens ook vragen te stellen aan uw *Chief Information Security Officer* (CISO). Een goede leidraad voor de relevante vragen vindt u in de NCSC-vragenlijst voor de bestuurder aan de CISO.[9]

Belangrijke vragen zijn:

- Wat zijn onze ICT-systemen en hebben we daar een actuele inventarisatie van? Hoeveel ongedocumenteerde ICT (*schaduw ICT*) hebben we?
- Wat zijn de belangrijkste dreigingen voor onze organisatie en waarom? Kijk daarbij naar aanvallers, hun tactieken en werkwijzen, maar ook naar het risico op onbedoelde verstoringen.
- Hebben we "legacy" systemen die niet meer onderhouden worden door de leverancier? Hebben we daarvoor een uitfaseringsplan en hoe beperken we ondertussen het risico?
- Hoe belangrijk is de cyberveiligheid van onze producten en diensten voor onze klanten of zelfs voor de maatschappij?
- Wat zijn onze belangrijkste 'controls' en wat is hun status?
- Wat is het gevolg van ontbrekende of niet-effectieve 'controls'? Hoe gaan we ze verbeteren?
- Worden onze belangrijkste ICT-systemen op weerbaarheid getest (red teaming)?
- Hebben we een incident response- en herstelplan? Testen we het?
- Hebben we een plan B mocht de ICT uitvallen? Wat zijn de uitwijkmogelijkheden?
- Hoe groot is ons restrisico? Valt dit binnen onze risicobereidheid?
- Hebben we zicht op belangrijke afhankelijkheden van ICT-leveranciers? Hoe beheersen we de risico's van die afhankelijkheid?
- Zijn de middelen die wij aan cyberbeveiliging toewijzen voldoende en effectief?
- Welke systemen zijn zo belangrijk voor ons dat we toegang sterk beperken, of zelfs alleen op fysieke locaties toestaan?
- Zijn we als bedrijf en als bestuurder (voldoende) verzekerd tegen cyberrisico's?
- Onder welke omstandigheden zijn we bereid om in te gaan op afpersing?
- Hoe staat het met de training van ons personeel in cyberveiligheid?
- Hoe is onze cyberbeveiliging ten opzichte van onze sectorgenoten?

De antwoorden zouden regelmatig (elk kwartaal) aan u moeten worden gerapporteerd, met context over belangrijke cyberincidenten binnen en buiten de organisatie, nieuwe dreigingen en ontwikkelingen op het gebied van regelgeving. De CISO dient bij die gelegenheid ook ontwikkelingen te signaleren die de situatie ten goede of ten kwade substantieel veranderen en relevante acties en middelen voorstellen.

7 https://www.digitaltrustcenter.nl/stappenplan-risicoanalyse
8 https://www.ncsc.nl/documenten/publicaties/2020/juli/21/factsheet-risicobeheersing
9 https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/besturen/vragen-voor-bestuurder-aan-ciso

5. PRIORITEIT STELLEN OM UW CYBERRISICO EFFECTIEF TE BEPERKEN

Als bestuurder wordt u verwacht de cyberrisico-strategie van uw organisatie goed te keuren en er toezicht op uit te oefenen. Nul risico is daarbij niet mogelijk en middelen zijn schaars. Gelukkig is het mogelijk om de cyberrisico-onderdelen te prioriteren en er op strategisch niveau toezicht op te houden zonder daarbij alle details te kennen.

Raamwerken, zoals ISO/IEC 27001[10], NIST CSF[11], COBIT[12], het NOREA DORA Framework[13] en het NIS2 Control Framework[14] zijn een nuttig hulpmiddel om cyberbeveiligingsrisico's te beheersen. Ze geven op een uitputtende manier aan welke organisatorische maatregelen en processen uw organisatie kan uitzetten om cyberveiligheid en weerbaarheid te borgen. Het maakt niet uit welk raamwerk uw organisatie kiest, als u intern maar **één enkel raamwerk** gebruikt in afstemming tussen CIO, CISO, en risico- en auditfuncties. Een leidraad voor het kiezen van een raamwerk vindt u op de website van het NCSC.[15]

Voor kleinere bedrijven waarvoor niet haalbaar is een raamwerk toe te passen, geeft een NCSC-leidraad de belangrijkste vijf basisprincipes van digitale weerbaarheid die handvatten geven voor het ontwikkelen van een cyberbeveiligingsstrategie.[16] Een waarschuwing is op zijn plaats. Raamwerken zijn met name georiënteerd op het borgen van **processen** (bijvoorbeeld: is er een **proces** voor uitwijk?) maar geven op zichzelf geen zekerheid dat het risico ook voldoende wordt gemitigeerd. Raamwerken toetsen dus niet de effectiviteit (werking) van de controls. Raamwerken omvatten meestal een proces voor goedkeuring van afwijking van voorgeschreven controls. Dan is aan het proces voldaan, maar is er dus nog geen sprake van het daadwerkelijk mitigeren van risico's. Een certificering onder een raamwerk geeft een beperkte mate van zekerheid.

Raamwerken bevatten verder honderden controls om alle aspecten van het beveiligings-risicobeheer in te richten. Niet alle controls zijn even belangrijk. De ervaring leert dat met een zeer beperkte subset van **key controls** de belangrijkste beveiligingsrisico's worden afgedekt.[17] Het meten van de goede werking van deze key controls alsook de effectiviteit ervan, stelt uw organisatie in staat om voor u een strategisch dashboard met *Key Control Indicators* (KCI's) op te zetten, zodat u goed geïnformeerd toezicht kan uitoefenen.

10 https://www.iso.org/isoiec-27001-information-security.html
11 https://www.nist.gov/cyberframework
12 https://www.isaca.org/resources/cobit
13 https://www.norea.nl/uploads/bfile/4693bb51-d6c0-4c3d-8e3e-577f74af9d73
14 https://www.norea.nl/regulatory
15 Ontdek het risicomanagementraamwerk dat bij jou past | Wat kun je zelf doen? | Nationaal Cyber Security Centrum
16 5 basisprincipes van digitale weerbaarheid | Wat kun je zelf doen? | Nationaal Cyber Security Centrum; op de website van het Digital Trust Center, is verder een CyberVeilig Check voor zzp en MMKB beschikbaar, de 5 basisprincipes van veilig digitaal ondernemen | Digital Trust Center (Min. van EZ).
17 https://www.digitaltrustcenter.nl/maak-je-mkb-bedrijf-cyberweerbaar

Hierna volgt een lijst met KCI's die is opgesteld door een werkgroep van CISO's van grote multinationals, en die als startpunt kan dienen voor het bepalen van de KCI's in uw organisatie.[18] De eerste KCI van deze lijst is verreweg de belangrijkste. Dit betreft het opzetten van een "Inventaris van ICT-systemen". Een organisatie kan immers niet iets beschermen waarvan je niet weet dat het bestaat. De andere KCIs zijn veelal gerelateerd aan de ICT-systemen in de inventaris. Bijvoorbeeld de KCI dat *back-ups* worden gemaakt of dat *beveiligingsupdates* worden geïnstalleerd, gelden alleen voor de ICT-systemen die in de inventaris zijn opgenomen. Deze KCI's worden minder zinvol als deze inventaris niet compleet is.

Tabel 1: Voorbeelden van Key Control Indicatoren

	Beschrijving	Meting
KCI 1	Inventaris van ICT-systemen	% kritische ICT-systemen in inventaris volgens beleid
KCI 2	Bevoorrechte toegangsrechten (*privileged access)*	% bevoorrechte toegangsrechten binnen beleid # bevoorrechte accounts
KCI 3	Oplossen van kwetsbaarheden	% hoog risico beveiligingsupdates binnen N uur
KCI 4	Betrouwbare back-ups van data en applicaties	Maximale tijd om belangrijke middelen te herstellen (% van kritieke middelen herstelbaar in N uur)
KCI 5	Beveiligde werkstations	% werkstations geconfigureerd in lijn met beleid
KCI 6	Logboeken verzamelen	% kritieke systemen ingericht voor logging
KCI 7	Netwerkbeveiliging	% conforme netwerkbeveiligingsinstellingen
KCI 8	Naleving door derden	% conforme belangrijke verbindingen met derden
KCI 9	Identiteitsbeheer	% dekking van systemen en gebruikers door aanmelding met meerdere factoren (MFA) % bevoorrechte accounts met *phishing resistant MFA*
KCI 10	Belangrijke incidenten	% grote cyberincidenten zonder bedrijfsimpact
KCI 11	Risicoaanvaarding	# risico geaccepteerde beleidsafwijkingen
KCI 12	Beveiliging van aan internet blootgestelde ICT-systemen	% aan internet blootgestelde bedrijfsmiddelen die voldoende beschermd en bewaakt zijn
KCI 13	Bewaking kroonjuwelen	% kroonjuwelen gedekt door beveiligingsmonitoring
KCI 14	Oorsprong van cyberincidenten	% beveiligingsincidenten gerelateerd aan tekortkomingen van minstens één essentiële controle
KCI 15	Weerbaarheidstesten	Resultaat van weerbaarheidstesten (*red teaming*)
KCI 16	Cryptografie	%middelen post-quantum beveiligd %middelen met compliant sleutelbeheer

18 https://www.researchgate.net/publication/374061802_Ten_Key_Insights_for_Informed_Cyber_Oversight

KCI's drukken de prioriteiten van de organisatie uit en de selectie ervan en rapportage daarover zal de richting van uw organisatie bepalen. De keuzes zijn dus cruciaal en het bestuur dient er een grondig gesprek over te voeren en besluiten over te nemen.

Vergeet hierbij niet om in industriële omgevingen ook de situatie rond operationele technologie en procesautomatisering (OT) in kaart te brengen. Bij OT is vaak sprake van verouderde software, die niet meer wordt onderhouden of waarvan het installeren van beveiligingsupdates van besturingssoftware tijdens de productie moeilijk is. Andere beschermingsmaatregelen dienen dan te worden genomen (bijv. isolatie), die aparte rapportage vereisen.

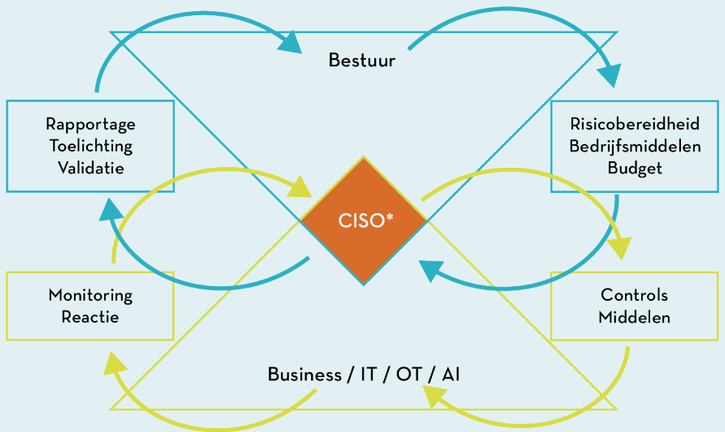
Wees verder voorzichtig met het gebruik van gemiddelden, deze kunnen belangrijke risico's verbergen. Als bijvoorbeeld de KCI het percentage cyberincidenten zou berekenen op basis van **alle** cyberincidenten (laag, midden en hoog risico) dan kan de KCI rapporteren dat 95% is opgelost **zonder** bedrijfsimpact, terwijl een hoog-risico incident **met** belangrijke schadelijke impact onder de radar blijft.

Tot slot geldt dat uw organisatie dient te zijn voorbereid op extreme scenario's (no-ICT, uitval toeleverancier, ...). Aanbevolen wordt om de weerbaarheid en veerkracht van uw organisatie regelmatig testen door het houden van *table top*-oefeningen en externe cyberweerbaarheidstesten, zoals TLPT, TIBER, en ART.[19]

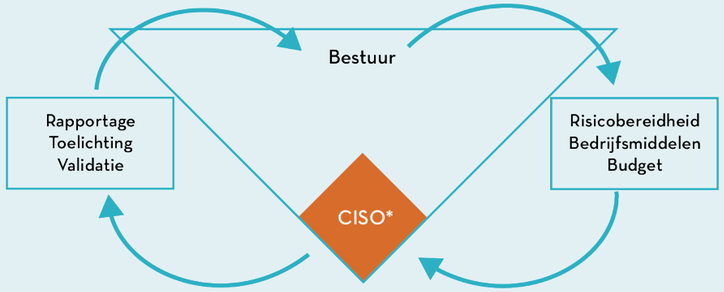
19 https://www.dnb.nl/voor-de-sector/betalingsverkeer/begeleiding-cyberweerbaarheidstesten-door-dnb/

6. CONTINU TOEZICHT – GOVERNANCE

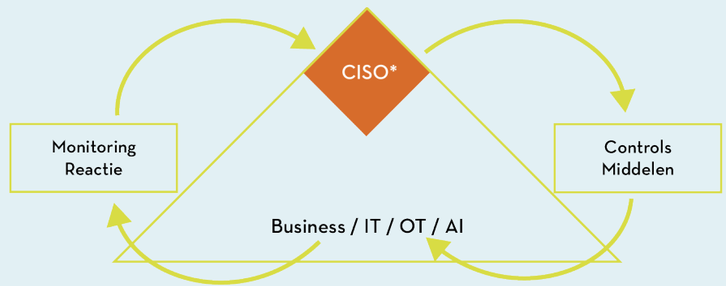
Voor traditionele bedrijfsrisico's bestaat er een gevestigde praktijk voor het rapporteren en toebedelen van verantwoordelijkheden. Voor het beheer van cyberbeveiligingsrisico's is er vaak nog geen gevestigde praktijk. Bijvoorbeeld is het lastig om de effectiviteit van cyberbeveiligingsprogramma's te meten en redelijke zekerheid te verkrijgen dat het restrisico binnen de risicobereidheid van de organisatie blijft. Gevolg is dat cyberrisico-rapportages aan bestuurders een grote verscheidenheid laat zien. Vaak gaat de rapportage over de voortgang in de implementatie van processen, waarbij *inspanningen* worden gemeten in plaats van *effectiviteit*.



Bovenstaande figuur illustreert een ideale situatie voor de *cyber governance*, de organisatie van besluitvorming, monitoring, rapportage en toezicht op het beheer van cyberbeveiligings-risico's. Uitgangspunt is dat organisaties een CISO (of vergelijkbare functionaris) aanstellen. De CISO neemt in de cyber governance een centrale positie in en is verantwoordelijk voor het ontwikkelen en uitvoeren van de maatregelen ter beheersing van de cyberbeveiligings-risico's. De CISO werkt hierbij nauw samen met de interne operationele diensten (business, ICT- en OT-operations, innovatie) en de risicobeheer- en auditfuncties.



In het bovenste gedeelte van de figuur ziet u dat de CISO de cyberbeheersmaatregelen afstemt met het bestuur in het bijzonder wat betreft risicobereidheid, bedrijfsprioriteiten en het cyberbudget. Het bestuur krijgt regelmatig informatie van de CISO over de status van de KCIs, het dreigingslandschap, belangrijke incidenten en ontwikkelingen in de regelgeving.



In het onderste gedeelte van de figuur ziet u dat de CISO de strategie van het bestuur doorvoert in de cyberbeheersmaatregelen, dit in samenwerking met de interne operationele diensten. De CISO controleert de effectiviteit van de cyberbeheersmaatregelen, reageert op afwijkingen en incidenten en past waar nodig aan. Veel activiteiten gebeuren in de onderste piramide en dus 'onder de motorkap' voor het bestuur.

Als bestuurder moet u ervoor zorgen dat uw CISO de vaardigheden, middelen, en autonomie heeft om het cybersecuritybeleid van de organisatie te ontwikkelen en implementeren en u te helpen bij het uitoefenen van goed geïnformeerd toezicht. Zorg er ook voor dat uw interne processen, verantwoordelijkheden en rapportagelijnen goed zijn vastgelegd in uw governance documentatie.

Het is belangrijk dat de CISO wordt ondersteund door een helder mandaat, voldoende doorzettingsmacht, en actieve medewerking van alle bedrijfsonderdelen.

Bevorder dat de rapportage van de CISO wordt gecoördineerd met de rapportages van risicobeheer en audit. Vraag ook om regelmatige rapportage en niet alleen in het geval van een incident. Zie erop toe dat de rapportage zich niet beperkt tot de *voortgang* in implementatie van processen, waarbij *inspanningen* worden gemeten in plaats van *effectiviteit*. Idealiter zou de CISO elk kwartaal persoonlijk verslag moeten uitbrengen aan het bestuur, en tussentijds als daartoe aanleiding is. Geef de CISO voldoende 'zendtijd'.

7. JURIDISCHE ASPECTEN VAN UW BESTUURS-VERANTWOORDELIJKHEID

Bestuurders hebben een algemene wettelijke plicht om hun taak behoorlijk te vervullen.[20] Daaronder valt het borgen dat de organisatie beschikt over adequaat werkende risicobeheersings- en controlesystemen.

Vanuit de EU zijn de verantwoordelijkheden van bestuurders van financiële instellingen en kritische infrastructuur aangescherpt in nieuwe richtlijnen en verordeningen - zoals NIS2,[21] CER,[22] en DORA.[23] Zij verplichten gereguleerde organisaties om maatregelen te treffen om cyberbeveiligingsrisico's te beheersen, en bepalen specifiek dat het de taak is van bestuurders om deze maatregelen goed te keuren, toe te zien op de uitvoering ervan en dat bestuurders daarvoor ook aansprakelijk kunnen worden gehouden. Ook stellen zij eisen aan de opleiding, kennis en expertise van bestuurders.

De impact van de nieuwe wettelijke bepalingen is verstrekkend. Zij vereisen in bijna alle organisaties een herziening van de bestaande risicobeheersings- en controlesystemen, inclusief die van de toeleveringsketen, evenals een explicitering van de *cyber governance* (bepalen van rollen, verantwoordelijkheden en bevoegdheden en rapportage structuren).

Als uw organisatie producten met een digitale component verkoopt (hardware, software, IoT-producten maar ook apps voor besturing van producten), moeten die vanwege de CRA[24] op termijn ook aan strenge cyberveiligheidseisen te voldoen.

Klik door naar meer over: NIS2, CER, DORA, CRA

20 Art. 9(1) Boek 2 BW

21 Network and Information Security Directive (NIS2), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

22 Critical Entities Resilience Directive (CER), 2022/2557 - EN - CER - EUR-Lex

23 Digital Operational Resilience Act (DORA), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

24 CRA https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202402847

Verantwoordelijkheden bestuurders onder NIS2 en DORA

Zowel NIS2 als DORA bepalen dat de gereguleerde entiteiten over adequate cyberrisico-beheersing dienen te beschikken, en specificeren welke risicobeheersingsmaatregelen minimaal moeten worden getroffen.

Bestuurders hebben de plicht om:

- De risicobeheersingsmaatregelen goed te keuren;
- Toe te zien op de uitvoering van deze maatregelen;
- Door opleiding, voldoende kennis en vaardigheden te verwerven om cyberrisico's te kunnen identificeren, de cyberrisicobeheersing en impact daarvan te kunnen beoordelen, en in staat zijn rapportages over cyberrisico te beoordelen.

Aansprakelijkheden bestuurders onder NIS2 en DORA

Zowel NIS2 als DORA bevatten bepalingen waarin personen in de organisatie persoonlijk aansprakelijk kunnen worden gesteld. In de publiciteit rondom NIS2 en DORA is daar veel aandacht voor, terwijl de werkelijke uitbreiding van aansprakelijkheid onder de nieuwe wetgeving vooral een gevolg is van het feit dat de taken en verantwoordelijkheden van de bestuurders nu specifiek zijn beschreven.

Indien deze taken niet voldoende worden vervuld, zal het voor bestuurders lastig zijn aan te tonen dat zij aan hun wettelijke plicht van behoorlijk bestuur hebben voldaan. Waar de verantwoordelijkheden van bestuurders specifieker zijn, geldt dit ook voor het toezicht op taken van raden van bestuur en toezicht.

Eerste inzicht voor bestuurders is dat de eindverantwoordelijkheid voor het beheer van en het toezicht op cyberrisico's niet kan worden gedelegeerd aan gespecialiseerde leidinggevenden, noch aan een gespecialiseerde (audit)commissie.

Er is sprake van een **collectieve verantwoordelijkheid** van het bestuur, waarbij individuele bestuurders hoofdelijk aansprakelijk kunnen worden gesteld voor verantwoordelijkheden van het bestuur als geheel, ook als bepaalde taken worden gedelegeerd aan specifieke leden van het bestuursorgaan.

Tweede inzicht is dat voor handhaving van (implementatie)bepalingen onder NIS2 en DORA de Algemene wet bestuursrecht relevant is. Dit betekent dat als een rechtspersoon een overtreding begaat, degene die tot **het feit opdracht heeft gegeven** of degene die **feitelijk leiding heeft gegeven** zelf ook bloot kan staan aan correctieve maatregelen, zoals oplegging van bestuurlijke boetes, een last onder bestuursdwang of dwangsom.

8. VERANTWOORDELIJKHEID VOOR CYBERRISICO'S IS NIET BEPERKT TOT UW EIGEN ORGANISATIE

Uw organisatie maakt deel uit van een toeleveringsketen. De cyberveiligheid van uw ICT is afhankelijk van die van uw leveranciers. Uw klanten zijn op hun beurt afhankelijk van de cyberveiligheid van uw producten en diensten. Uw beheer van het cyberrisico is daarom niet beperkt tot uw eigen organisatie.

Breid uw toezicht uit naar uw *toeleveringsketen*, geef daarbij prioriteit aan leveranciers of dienstverleners die kritisch zijn voor uw organisatie, en mitigeer hun cyberrisico. Zij kunnen ook een doelwit zijn van cybercriminelen en uw organisatie mogelijk een onbedoeld slachtoffer.

Het is ook raadzaam dat u de leveranciers laat beoordelen naar technische afhankelijkheid (*vervangbaarheid*) en ongewenste geopolitieke afhankelijkheden. Voorkom echter overdaad in controlevereisten indien de leveranciers of dienstverleners weinig kritisch zijn voor uw organisatie en processen.

De Europese wetgever heeft de beveiliging van het cyberrisico in uw rechtstreekse leveranciers en dienstverleners opgenomen als onderdeel van de zorgplicht in NIS2 en DORA. Onderliggende strategische keuze van deze wetgeving alsook van de Nederlandse Cyber Security Strategie[25] is dat "groot" zich inzet om "klein" te helpen bij hun cyberrisicobeheersing.

Zorg dat uw eigen digitale producten wat betreft ontwerp, configuratie en gebruik veilig zijn (security-by-design en security-by-default), bij voorkeur ondersteund door een certificaat.

Indien uw organisatie producten met een digitale component verkoopt (hardware, software, IoT-producten maar ook apps voor besturing van producten), breid dan uw toezicht uit naar deze producten en beperk het cyberrisico voor uw klanten door te borgen dat het ontwerp, configuratie en gebruik veilig zijn (*security-by-design en security-by-default*). Houd bij uw toezicht ook rekening met de eventuele maatschappelijke impact die een incident in uw organisatie zou kunnen teweegbrengen.

De Europese wetgever heeft de beveiliging van het cyberrisico voor uw eigen producten met digitale component opgenomen als onderdeel van de zorgplicht in de CRA. Dit zal in positieve zin bijdragen aan de digitale weerbaarheid van bedrijven en consumenten.

25 Zie onderliggende strategische keuzes p. 18-19, Nederlandse+Cybersecuritystrategie+2022-2028 (1).pdf

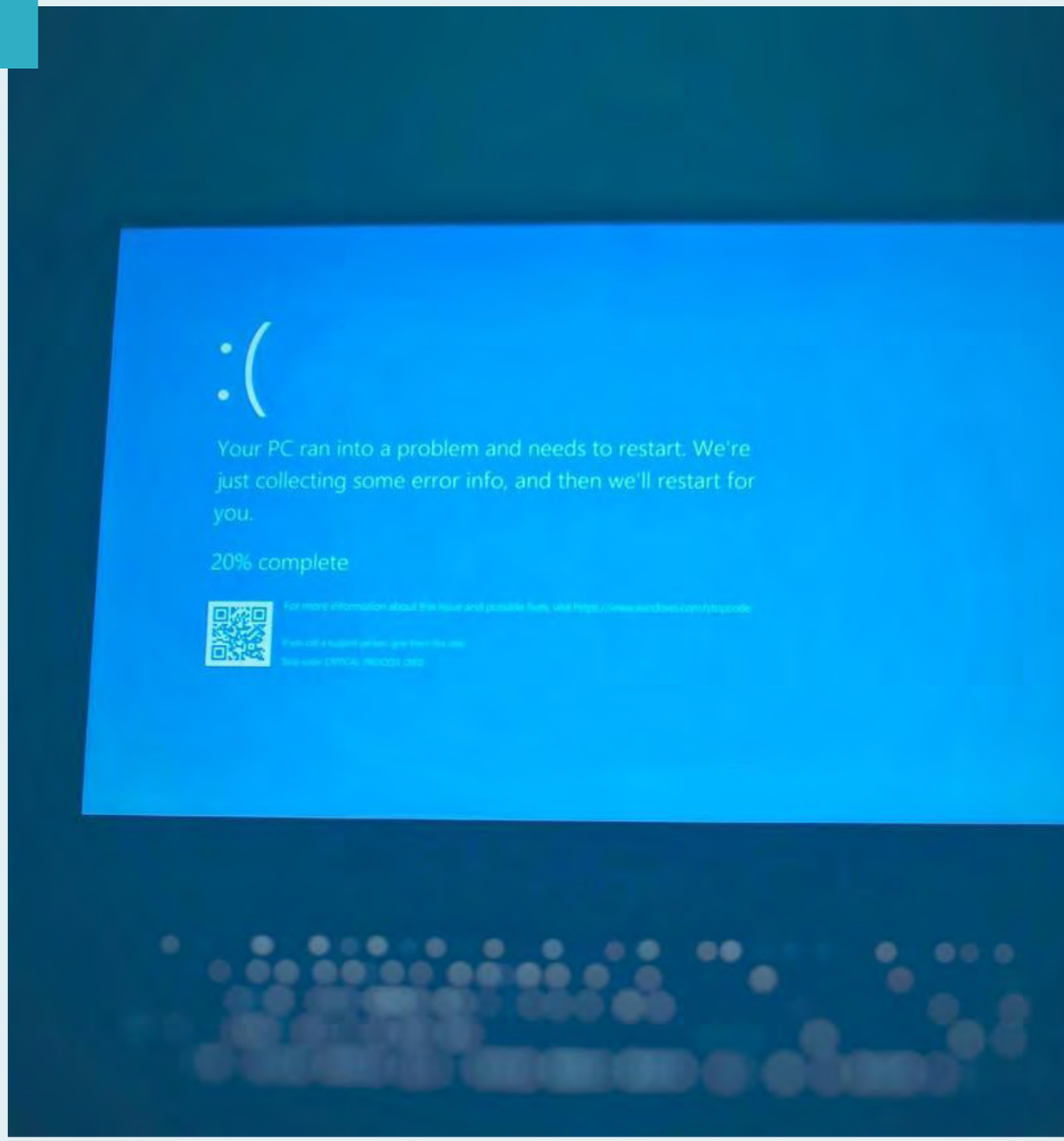
9. EXTERNE RAPPORTAGE-VERPLICHTINGEN

Uw organisatie heeft ook externe cybersecurity rapporteringsverplichtingen zoals:

- Toezichthouders op de regelgeving waaronder uw organisatie valt;
- Accountants die uw jaarrekening controleren, aandeelhouders, de financiële markt;
- Afnemers;
- Verzekeraars.

De bouwstenen van deze externe rapporteringsverplichtingen zijn vergelijkbaar met die van het raamwerk dat intern door uw organisatie wordt toegepast. Om de vertaalslag te maken tussen uw interne raamwerk en de raamwerken die uw externe stakeholders gebruiken, zijn zogenaamde '*mappings*' beschikbaar, zoals het CRI Profile.[26] Tevens zijn er initiatieven die geïntegreerde rapportage over de ICT-beheersing mogelijk maken, zoals de International Digital Reporting Standard (IDRS).[27]

Bij het toepassen van een *mapping*, dient u erop toe te zien dat uw organisatie in de externe rapportage voldoende context aanbrengt en coherent de elementen rapporteert die de externe partij verwacht.



26 https://cyberriskinstitute.org/

27 International Digital Reporting Standards, Governance of IT, version 2.1, May 2025

10. BESTUURDERSTRAINING MET IMPACT

De praktijk wijst uit dat training van bestuurders een belangrijke impact kan hebben op een organisatie. De training moet dan wel verder gaan dan het leveren van theoretische inhoud. Bestuurders, commissarissen en toezichthouders hoeven geen technische experts te worden. Het doel van de training is niet om u op te leiden tot een “CISO-light”, maar om u in staat te stellen geïnformeerd een strategische discussie te voeren en het nodige toezicht uit te oefenen. Belangrijke onderwerpen die aan de orde moeten komen zijn:

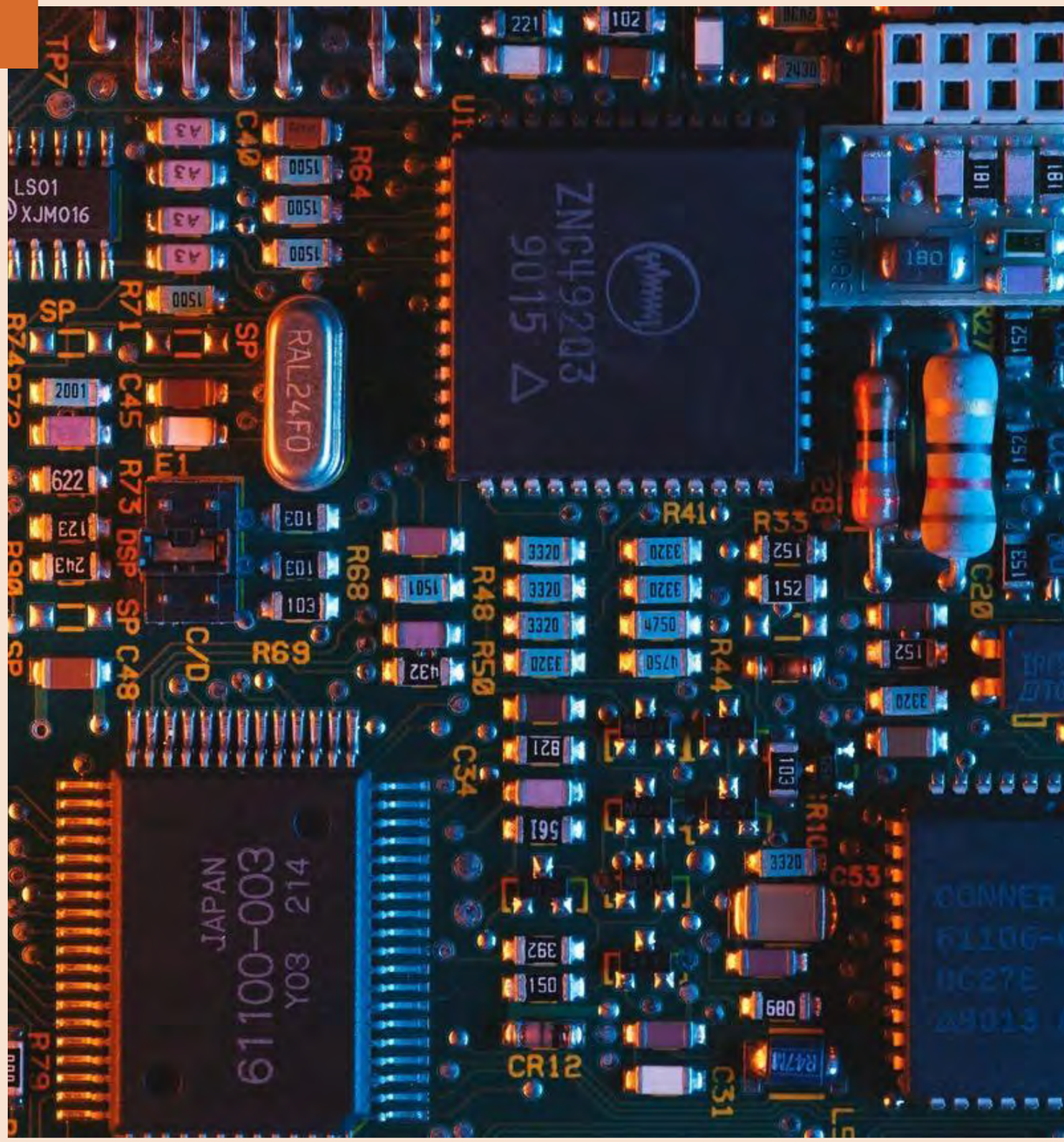
- Relevante elementen in de cyberregelgeving, zowel in de EU als daarbuiten;
- Rol en verantwoordelijkheid van bestuurders;
- Het nut en de beperkingen van raamwerken;
- Hoe het beste een internationaal programma voor cyberrisicobeheer op te zetten om te zorgen dat gemaakte inspanningen ook elders kunnen worden benut;
- Goede cyber governance (rol van CISO, wie rapporteert wat aan wie en hoe vaak?);
- Wat is onze cyber risicobereidheid (*risk appetite*)?
- Wat zijn de belangrijkste ‘controls’ en hoe meten we die?
- Gap-analyse van het huidige cyberrisicobeheer en de gewenste situatie;
- Instellen van een continu verbeteringsproces (*Plan-Do-Check-Act*).

Als deze strategische elementen goed aan de orde zijn gekomen, kan het bestuur ‘in positie’ komen en de nodige wijzigingen aanbrengen in de governance en bestuursrapportage om ervoor te zorgen dat u toezicht kan houden.

Enkele praktische tips bij het organiseren van een cybertraining voor bestuurders[28]:

- Geef de training op kantoor, fysiek, als een agendapunt tijdens een reguliere vergadering van het bestuur;
- Nodig ook uw CIO, CISO, hoofd risk, auditor en hoofd juridische zaken uit, zodat alle relevante verantwoordelijken dezelfde boodschap krijgen;
- In veel gevallen zal de huidige cyber governance en de rapportage aan bestuurders nog niet aan de ideale situatie voldoen. Gebruik de voorbereiding van de training om eventuele interne wrijvingen en onenigheid tussen de verschillende afdelingen te bespreken en te adresseren;
- Stem de inhoud van de training af op uw organisatie, uw infrastructuur, uw sector, en uw huidige governance- en rapportage;
- Maak voldoende tijd vrij (2-3 uur) om ook inhoudelijk het gesprek te starten over de risicobereidheid, belangrijkste controls, rapportageprocessen en governance;
- Gebruik de training als een (continu) verbeterinstrument voor uw organisatie.

28 Gebruik bijvoorbeeld de guideline boardroomtraining van NOREA

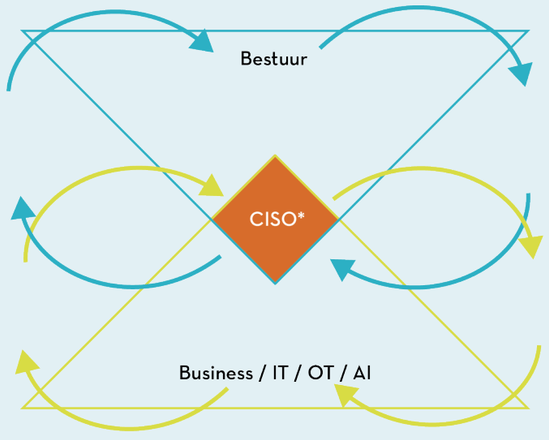


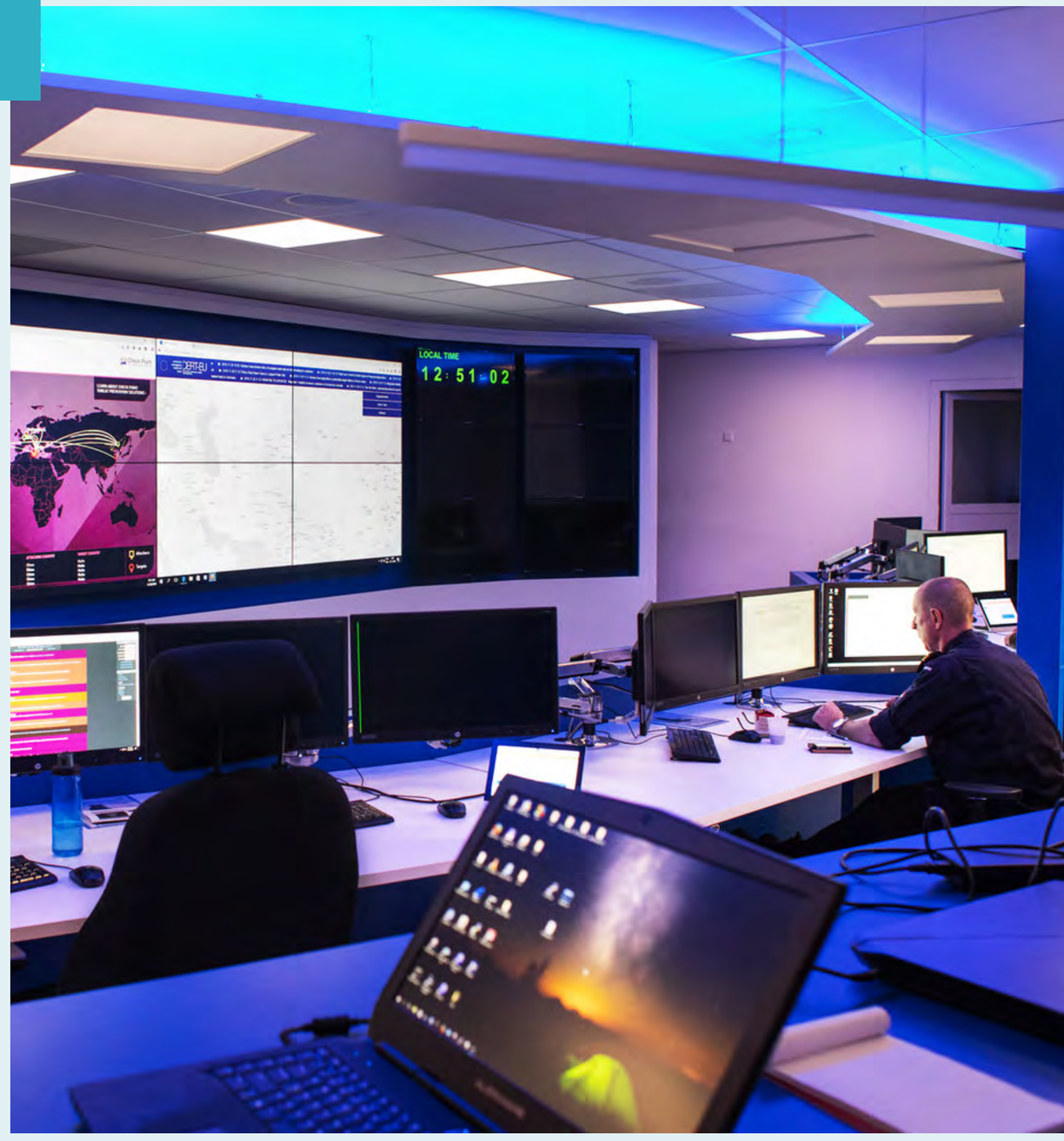
11. HOUD DE VINGER AAN DE POLS EN VERBETER WAAR NODIG

U moet er niet van uitgaan dat cyberrisico's statisch zijn. Uw organisatie, uw infrastructuur en het dreigingslandschap ontwikkelen zich voortdurend. Technologische ontwikkelingen zoals AI, quantum computing en Internet of Things, introduceren nieuwe risico's en vergen tijdige aanpassing van uw beveiligingsstrategie.

Het is daarom van belang dat u ervoor zorgt dat uw processen en beveiligingsmaatregelen periodiek worden geëvalueerd en aangepast aan alle ontwikkelingen om te borgen dat de risico's binnen uw risicobereidheid blijft. Het beheer van het cyberrisico dient daarom deel uit te maken van een continu verbeteringsproces. Doel is borging van de bedrijfscontinuïteit en dat van de gehele keten.

Figuur 3: Continu verbeteren





12. DE JUISTE TOON AAN DE TOP - GEEF HET GOEDE VOORBEELD

Wees u ervan bewust dat u zelf een mogelijk doelwit bent van cybercriminelen. U heeft toegang tot waardevolle bedrijfsmiddelen. Cyberbeveiliging zou daarom voor uzelf een vanzelfsprekendheid moeten zijn, zoals een strikte scheiding van laptop en mobiele telefoons voor werk en privégebruik, toepassen van MFA, en gebruik van een applicatie om uw wachtwoorden te beheren. Dit is noodzakelijk om het risico te beperken dat u voor uw organisatie kan creëren, maar uw houding zal ook een positief effect hebben op de manier waarop uw medewerkers zich zullen gedragen. Goede cyberveiligheid begint aan de top.Deze handreiking is een product van de Cyber Security Raad.

13. DANKWOORD

Deze handreiking is een product van de Cyber Security Raad. Onze dank gaat uit naar de auteurs van deze handreiking en de organisaties die hun medewerking hebben verleend.

Auteurs:
- Lokke Moerel (hoogleraar Global ICT Law Universiteit Tilburg en CSR lid namens de wetenschappelijke sector)
- Freddy Dezeure (onafhankelijk adviseur)

Met medewerking van de volgende personen en organisaties:

- Sabine Gielens (namens VNO-NCW en MKB-Nederland)
- Michiel Steltman (namens ECP)
- Liesbeth Holterman (namens Cyber Veilig Nederland)
- Marlou Snelders (namens FME)
- Ronald Verbeek (namens het CIO Platform)
- Eelco Stofbergen (namens NLdigital)
- Pieter van den Berg (namens de Nationaal Coördinator Terrorismebestrijding en Veiligheid)
- Tim Puts (namens het ministerie van Defensie)

BIJLAGEN

BIJLAGE 1:
LIJST VAN AFKORTINGEN EN TERMINOLOGIE

CISO	Chief Information Security Officer of vergelijkbare functionaris
CIO	Chief Information Officer
ICT	Informatie- en Communicatietechnologie, in deze handreiking gebruiken we ICT als in zijn breedste definitie om alle vormen van informatietechnologie te benoemen
OT	Operationele Technologie
IoT	Internet of Things
NIS2	Network and Information Security Directive (EU)
CER	Critical Entities Resilience Directive (EU)
DORA	Digital Operational Resilience Act (EU)
CRA	Cyber Resilience Act (EU)
Control	Risicobeperkende maatregel
KCI	Key Control Indicator
Raamwerk	document dat richtlijnen, standaarden en best practices bevat die helpen om cybersecurity risico's te mitigeren
Awb	Algemene wet bestuursrecht (NL)
DNB	De Nederlandsche Bank (NL)
AFM	Autoriteit Financiële Markten (NL)
MFA	Multi-factor authenticatie, vereist meerdere verificatiefactoren voor aanmelding
Phishing resistant MFA	MFA met bijkomende beveiliging om "phishing" van verificatiefactoren te verhinderen

Referenties

Tien belangrijke inzichten voor geïnformeerd cybertoezicht
Cyberrisico's rapporteren aan raden van bestuur, bestuursuitgave
Cyberrisico's rapporteren aan Raden van Bestuur, CISO-uitgave

BIJLAGE 2:
NIET-UITPUTTENDE LIJST VAN CYBERRISICO'S

- ✓ Onderbreking van de continuïteit van bedrijfsprocessen zoals productie van goederen, administratie, toegang tot gebouwen, logistiek, communicatie met de buitenwereld, beschikbaarheid van de website.
- ✓ Ongeoorloofde toegang tot persoonsgegevens (privacy) van werknemers, klanten, burgers, patiënten etc.
- ✓ Afpersing als gevolg van een ransomwareaanval of een dreiging van publiek maken van vertrouwelijke gegevens.
- ✓ Rechtstreeks financieel verlies door misleiding van werknemers met toegang tot financiële middelen, misbruik van financiële processen, vervalsing in de facturatieketen.
- ✓ Reputatieschade en verlies aan vertrouwen vanwege klanten of burgers door het bekend worden een cyberaanval op de organisatie.
- ✓ Reputatieschade door overname van officiële communicatiekanalen door onbevoegden.
- ✓ Reputatieschade en productaansprakelijkheid schade door gecompromitteerde producten of diensten.
- ✓ Strategische schade door verlies van geheime gegevens aan geopolitieke tegenstanders, door verlies van bedrijfsgeheimen aan concurrenten, verlies van vertrouwelijke juridische informatie.
- ✓ Ongevallen met slachtoffers of materiële schade door gecompromitteerde producten of diensten in de medische sector, transportsector etc.
- ✓ Financieel verlies door de kosten van incident response en herstel van de infrastructuur.
- ✓ Financiële kosten van juridische gevolgen van een incident zoals geschillen met klanten, met regelgevende instanties, met verzekeringen.

BIJLAGE 3:
CHECKLIST VOOR BESTUURDERS

- ✓ Organiseer “all-hands” training voor bestuurders om geïnformeerde besluitvorming en toezicht op uitvoering van cyberrisicobeheersing mogelijk te maken. Vraag uw CISO het dreigingslandschap voor uw organisatie in kaart te brengen.
- ✓ Bepaal uw cyber risicobereidheid (*risk appetite*).
- ✓ Vraag om de cyberrisico-strategie en de maatregelen voor het beheersen van cyberbeveiligingsrisico’s op te stellen, voor te leggen en keur deze daarna formeel goed.
- ✓ Vraag om de top KCIs voor te stellen, doelstellingen vast te leggen, te meten en te rapporteren op kwartaalbasisOrganiseer en test het incident respons- en herstelplan.
- ✓ Pas uw cyber governance aan met heldere mandaten en rapportage lijnen voor het uitzetten, monitoren en rapporteren van de cyberrisico-strategie. Voorzie daarin voldoende middelen, autonomie en ondersteuning voor de CISO.
- ✓ Vraag om relevante regelgeving voor uw organisatie in kaart te brengen en een plan om aan de vereisten te voldoen.
- ✓ Bepaal welke personen/functies onder toepasselijke regelgeving aansprakelijk kunnen worden gesteld en organiseer een aangepaste aansprakelijkheidsverzekering.
- ✓ Check of u alle relevante vragen aan uw CISO heeft gesteld.

BIJLAGE 4:
MEER INFORMATIE OVER SPECIFIEKE NEDERLANDSE WETTELIJKE VOORSCHRIFTEN

Lees meer over NIS2 – Cyberbeveiligingswet

De NIS2-richtlijn richt zich op entiteiten in sectoren die al onder de eerste NIS-richtlijn vielen en entiteiten in nieuwe sectoren. Organisaties die onder de toepasselijkheid van de richtlijn (en daarmee de hieronder genoemde Cyberbeveiligingswet) vallen zijn op grond van de daarin bepaalde criteria ‘essentiële’ of ‘belangrijke’ entiteit. De Rijksinspectie Digitale Infrastructuur (RDI) heeft een zelfevaluatie[29] ontwikkeld waarmee organisaties zelf kunnen inschatten of ze onder de Cyberbeveiligingswet vallen en of zij worden gezien als “essentieel” of “belangrijk”.

NIS2 is een Europese richtlijn en dient in Nederlands recht te worden omgezet voordat het in de richtlijn bepaalde van kracht wordt. In Nederland wordt de NIS2-richtlijn geïmplementeerd in een nieuwe wet - de *Cyberbeveiligingswet* - waarvan het wetsontwerp is gepubliceerd op 11 december 2024.[30]

De Cyberbeveiligingswet wordt nader uitgewerkt in een algemene maatregel van bestuur – het *Cyberbeveiligingsbesluit* – waarvan de internetconsultatie op 30 maart 2025 sluit,[31] alsook in ministeriële regelingen die hun basis vinden in de wet of het besluit. In het besluit worden bepaalde onderwerpen uit de Cyberbeveiligingswet nader uitgewerkt, zoals de zorgplicht, registratieplicht en trainingsplicht voor bestuurder.

Deze handreiking zal worden aangepast indien daartoe aanleiding is als de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit definitief worden. De verwachting is dat dit niet eerder dan eind 2025 zal plaatsvinden.

NIS2 Cyberbeveiligingswet – Verantwoordelijkheden bestuurders

Artikel 21 (zorgplicht) Cyberbeveiligingswet bepaalt dat de gereguleerde entiteiten “passende en evenredige technische, operationele en organisatorische maatregelen dienen te nemen om de risico’s voor de beveiliging van de netwerk- en informatiesystemen, die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruikt, te beheersen. Ook neemt zij deze maatregelen om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van haar diensten en voor andere diensten te beperken.”

29 https://regelhulpenvoorbedrijven.nl/NIS-2-NL/
30 Cyberbeveiligingswet | Overheid.nl | Wetgevingskalender
31 Overheid.nl | Consultatie Cyberbeveiligingsbesluit

Op grond van **art. 26 Cyberbeveiligingswet** dient het bestuur:

- De maatregelen bedoeld in art. 23 goed te keuren.
- Toe te zien op de maatregelen en de uitvoering daarvan.
- Kennis en vaardigheden te hebben en deze actueel te houden.

Artikel 21 zelf geeft geen opsomming van de maatregelen zoals opgenomen in Artikel 21 NIS2. De Cyberbeveiligingswet bepaalt dat deze maatregelen zullen worden gespecificeerd bij algemene maatregel van bestuur, hetgeen is gedaan in Hoofdstuk 4 (zorgplicht) van het Cyberbeveiligingsbesluit. De uitwerking daar dekt alle maatregelen van Artikel 21 NIS2, maar is op sommige onderwerpen iets specifieker.

NIS2 Cyberbeveiligingswet – Toeleveringsketen vereisten

Wat betreft de maatregelen ten aanzien van de toeleveringsketen bepaalt Artikel 10 van het Cyberbeveiligingsbesluit dat het beleid dient toe te zien op afhankelijkheden van producten en diensten van rechtstreekse leveranciers voor zover die invloed kunnen hebben op de beveiliging van de netwerk- en informatiesystemen van uw eigen organisatie.[32]

NIS2 Cyberbeveiligingswet - Aansprakelijkheden bestuurders

NIS2 voorziet in twee gevallen waarin personen in de organisatie persoonlijk aansprakelijk kunnen worden gesteld.

Collectieve aansprakelijkheid. *De bestuursorganen kunnen aansprakelijk worden gesteld voor het niet treffen van de maatregelen door de entiteit voor het beheer van cyberbeveiligingsrisico's.*

Aansprakelijkheid wordt toegerekend aan 'bestuursorganen' als geheel, wat wijst op collectieve verantwoordelijkheid, waarbij individuele leden hoofdelijk aansprakelijk kunnen worden gesteld voor verantwoordelijkheden van het bestuur als geheel, ook als bepaalde taken worden gedelegeerd aan specifieke leden van het bestuursorgaan.

Individuele aansprakelijkheid. *Elke natuurlijke persoon die verantwoordelijk is voor of optreedt als wettelijk vertegenwoordiger van een gereguleerde entiteit, kan aansprakelijk worden gesteld voor schending van zijn verplichtingen om de naleving van NIS2 te waarborgen.*[33]

"Wettelijke vertegenwoordiging" wordt uitgelegd op basis van de volgende kenmerken van de natuurlijke persoon:

- bevoegdheid om de entiteit te vertegenwoordigen;
- bevoegdheid om namens de entiteit beslissingen te nemen;
- bevoegdheid om controle uit te oefenen op de entiteit.

32 Zie p. 10 van de Nota van Toelichting bij de consultatieversie van het Cyberbeveiligingsbesluit.
33 Artikel 32 lid 6, in samenhang met artikel 33 lid 5 NIS2.

Individuele aansprakelijkheid is hier dus niet beperkt tot bestuurders. De bepaling heeft ook betrekking op personen onder het hoogste bestuursniveau (d.w.z. ook werknemers, zoals een CISO), op voorwaarde dat de betreffende werknemer de relevante verantwoordelijkheden en bevoegdheden heeft gekregen. Dit kan bijvoorbeeld van toepassing zijn op de CISO, waar deze bevoegd is om beslissingen te nemen in het kader van NIS2-compliance, zoals het offline halen van het netwerk in geval van een beveiligings-incident of het melden van een beveiligingsincident aan de bevoegde autoriteit.

In NIS2 is niet nader gespecificeerd welk type of welke omvang van de aansprakelijkheid is bedoeld (civiel, administratief, strafrechtelijk), en een dergelijke specificatie zal dus in het nationale recht moeten worden opgenomen. Het wetsvoorstel Cyberbeveiligingswet voorziet in bestuursrechtelijke handhaving waarop de Algemene wet bestuursrecht van toepassing is. Het wetsvoorstel bevat geen bepalingen die specifiek over aansprakelijkheid van individuele personen gaan.[34] Uit de Memorie van Toelichting[35] bij het wetsvoorstel blijkt dat de Algemene wet bestuursrecht dit al afdoende reguleert. Hieruit volgt dat als een rechtspersoon een overtreding begaat, degene die tot het *feit opdracht heeft gegeven* of degene die *feitelijk leiding* heeft gegeven zelf ook bloot kan staan aan correctieve maatregelen, zoals oplegging van bestuurlijke boetes, een last onder bestuursdwang of dwangsom.

Het voorgaande geldt niet onverkort vooraansprakelijkheid van overheidsinstanties, ambtenaren en verkozen of benoemde overheidsfunctionarissen. Die kan op onderdelen afwijkend zijn. NIS2 laat hiervoor uitdrukkelijk de ruimte.

De Memorie van Toelichting gaat niet specifiek in op civielrechtelijke bestuurdersaansprakelijkheid in het kader van het Burgerlijk Wetboek, waarmee de conclusie is dat de algemene regels inzake (interne en externe) aansprakelijkheid van bestuurders in het Nederlandse burgerlijk recht gelijk blijven.

Hoewel geen aansprakelijkheidsbepaling, bepaalt NIS2 dat in zeer uitzonderlijke omstandigheden de algemeen directeur of andere persoon met leidinggevende verantwoordelijkheden op het niveau van de wettelijke vertegenwoordiger tijdelijk kan worden geschorst van de uitoefening van leidinggevende functies.35 Een dergelijke schorsing moet op verzoek van een toezichthoudende autoriteit door een rechtbank worden opgelegd. De mogelijkheid tot tijdelijke schorsing geldt niet voor de bestuurders van overheidsinstanties.

34 Artikel 20, 32 lid 6 en artikel 33 lid 5 van NIS2.
35 *9248e519-467c-4323-873a-2dcdd47d3948_1.pdf, zie paragraaf 5.6.7.

NIS2 Cyberbeveiligingswet - Trainingsvereisten

De Cyberbeveiligingswet vereist dat iedere bestuurder binnen twee jaar na inwerkingtreding van de wet beschikt over de kennis en vaardigheden om:

- risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren;
- risicobeheersingsmaatregelen op het gebied van cyberbeveiliging te kunnen beoordelen;
- de gevolgen van de risico's en risicobeheersingsmaatregelen voor de diensten die door de entiteit worden verleend te kunnen beoordelen.

Bestuurders dienen deze vaardigheden aantoonbaar actueel te houden en certificaten van deelname aan gevolgde te kunnen overleggen. Het Cyberbeveiligingsbesluit specificeert dit nog verder door te bepalen dat de training in ieder geval de volgende onderwerpen dient te behandelen:

- de soorten risico's voor netwerk- en informatiesystemen;
- de risicomanagementprocessen;
- risicobeoordelingsmethodiek;
- de risicobeheersingsmaatregelen (zie Art. 21 Cyberbeveiligingswet) die het bestuur wordt geacht goed te keuren en toezicht te houden op uitvoering ervan.

Geen eisen worden gesteld aan de duur van de training.

Lees meer over DORA

De Digital Operational Resilience Act (DORA) is Europese wetgeving die als doel heeft om de digitale weerbaarheid van de financiële sector te vergroten. DORA omvat een *verordening* en een *richtlijn*.[36] Een verordening werkt rechtstreeks door in de Nederlandse rechtsorde en is per 17 januari 2025 in werking getreden. Wel moet worden voorzien in uitvoering en handhaving van de verordening. Dat is gebeurd met een wijziging van het *Besluit uitvoering EU-verordeningen financiële markten*, waarmee DNB en de AFM als bevoegde autoriteiten met de uitvoering en handhaving van de DORA verordening zijn belast.[37]

Op 17 januari 2025 zijn tevens in werking getreden de implementatiewet van de DORA richtlijn, waarbij ook een aantal bepalingen in de Wet op het financiële toezicht is aangepast die niet strookten met de DORA verordening[38], en het *Implementatiebesluit digitale operationele weerbaarheid financiële sector*. De drie Europese Toezichthoudende Autoriteiten (ESA's) zijn gezamenlijk aangewezen om de ontwikkeling van de technische standaarden voor DORA te leiden, waarvan er inmiddels een aantal zijn gepubliceerd.[39]

36 Richtlijn (EU) 2022/2556 betreffende een kader voor digitale operationele weerbaarheid van de financiële sector.

37 Meer specifiek door wijziging van bijlage 35 bij het Besluit uitvoering EU-verordeningen financiële markten.

38 Implementatiewet DORA, houdende wijziging van de Wet op het financieel toezicht ter implementatie van Richtlijn (EU) 2022/2556 betreffende een kader voor digitale operationele weerbaarheid van de financiële sector.

39 Zie voor overzicht technische standaarden: DORA | De Nederlandsche Bank

DORA - Verantwoordelijkheden bestuurders

Artikel 5 DORA legt de volgende verplichtingen op aan financiële entiteiten:

- Financiële entiteiten dienen te beschikken over een intern governance- en controlekader dat een doeltreffend en prudent beheer van het ICT-risico waarborgt.
- Het 'leidinggevend orgaan' dient alle regelingen met betrekking tot het kader voor ICT-risicobeheer te bepalen, deze goed te keuren en toezicht te houden op de uitvoering ervan. Art. 5 lid 2 sub (a) bepaalt vervolgens uitdrukkelijk dat het leidinggevend orgaan is belast met "de eindverantwoordelijkheid voor het beheer van het ICT-risico van de financiële entiteit". Onder 'leidinggevend orgaan' wordt verstaan zowel het bestuur als de raad van commissarissen.[40]
- De leden van het leidinggevend orgaan dienen actief voldoende kennis en vaardigheden te onderhouden om ICT-risico's en de gevolgen daarvan voor de verrichtingen van de financiële entiteit te begrijpen en te beoordelen, onder meer door regelmatig specifieke opleidingen te volgen die in verhouding staan tot het te beheren ICT-risico's.

Voor bestuurders en commissarissen geldt dat kennis van DORA inmiddels een onderwerp is dat meestal aan de orde komt in de geschiktheidsinterviews.

DORA – Aansprakelijkheden bestuurders

De bevoegde autoriteiten kunnen de financiële entiteit bepaalde administratieve straf- en corrigerende maatregelen opleggen.[41] De DORA-verordening bepaalt vervolgens de bevoegde autoriteiten ook de bevoegdheid hebben om administratieve strafmaatregelen of corrigerende maatregelen te nemen ten aanzien van leden van het leidinggevend orgaan van de financiële entiteit en andere personen die krachtens nationaal recht verantwoordelijk zijn voor de inbreuk.[42]

De DNB en de AFM zijn als bevoegde autoriteiten met de uitvoering en handhaving van DORA belast.[43] Zij mogen bij overtreding van voorschriften uit DORA een last onder dwangsom of een boete opleggen, en beschikken daarnaast ook over bevoegdheden die zijn neergelegd in de Wet op het Financieel Toezicht (Wft). Het handhavingsbeleid van AFM en DNB is met de komst van DORA niet aangepast.[44]

40 Zie voetnoot 9.

41 Artikel 50 lid 2, punt c, jo lid 4 en lid 5 DORA.

42 Artikel 50 lid 5 DORA.

43 Door wijziging van bijlage 35 bij het Besluit uitvoering EU-verordeningen financiële markten.

44 Zie voor het handhavingsbeleid en sanctiemogelijkheden van DNB en AFM: wetten.nl - Regeling - Het handhavingsbeleid van de AFM en DNB - BWBR0044284

Lees meer over CER

De CER-richtlijn richt zich op zogenaamde ‘kritieke’ entiteiten die essentiële diensten verlenen binnen de sectoren energie, drinkwater, vervoer, digitale infrastructuur, levensmiddelen, gezondheidszorg, infrastructuur voor de financiële markt, afvalwater, overheid, bankwezen en ruimtevaart. Voor ‘kritieke entiteiten’ gelden – in aanvulling op de cyberbeveiligingseisen onder NIS2 - tevens vereisten ter borging van de **fysieke weerbaarheid** van deze organisaties, bijvoorbeeld tegen sabotage.

De CER-richtlijn wordt geïmplementeerd in de *Wet weerbaarheid kritieke entiteiten*.[45] De ministeries die verantwoordelijk zijn voor de kritieke sectoren bepalen welke organisaties zij als kritieke entiteit aanwijzen. Dit hoeft een organisatie dus niet zelf te bepalen. De Wet weerbaarheid kritieke entiteiten wordt nader uitgewerkt in een algemene maatregel van bestuur - het *Besluit weerbaarheid kritieke entiteiten*, waarvan de internetconsultatie op 30 maart 2025 sluit.[46] Op de vereisten onder de CER/Wet weerbaarheid kritieke entiteiten wordt hierna niet verder ingegaan.

Lees meer over CRA

De Cyber Resilience Act (CRA)[47] is een Europese Verordening CRA stelt bindende eisen aan de cyberveiligheid van ‘alle producten met digitale elementen’ (alle hardware, software en IoT-apparaten), zodat consumenten en bedrijven veilig gebruik kunnen maken van digitale producten, denk aan webcams en smart-tv’s die deel uitmaken van het Internet of Things (IoT).

De wet dwingt bedrijven om cybersecurity niet langer als bijzaak, maar als kernonderdeel van hun productontwikkeling te beschouwen. Er is een overgangsperiode ingevoerd die eindigt op 11 december 2027, zodat producten en processen kunnen worden aangepast aan de nieuwe eisen. De overgangsperiode voor de meldplicht voor cyber security incidenten eindigt al eerder, per 11 september 2026. Op de vereisten onder de CRA wordt hier verder niet ingegaan.

45 Wet weerbaarheid kritieke entiteiten | Overheid.nl | Wetgevingskalender
46 Overheid.nl | Consultatie Besluit weerbaarheid kritieke entiteiten
47 https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202402847

September 2025

CSR Cyber Security Raad