De CISO in de praktijk

Werkboek voor bestuurders, toezichthouders en securityleiders

Inhoudsopgave (achter in het boek)

Het werkboek telt vier delen, achttien hoofdstukken en vier bijlagen. Elk hoofdstuk eindigt met een vast werkblok: samenvatting, reflectievragen, checklist, praktische opdrachten, template en do's en don'ts.

Woord vooraf en leeswijzer

Dit werkboek gaat over een functie die in veel organisaties nog zoekt naar haar plaats. Bijna iedere organisatie van enige omvang heeft iemand met de titel CISO, maar wat die persoon mag, moet en kan, verschilt sterk. Sinds de Cyberbeveiligingswet in Nederland en de NIS2-wet in België is cybersecurity bovendien uitdrukkelijk een verantwoordelijkheid van het bestuur. Daarmee is de positie van de CISO geen interne kwestie meer, maar een bestuurlijke.

Het boek is geschreven vanuit de praktijk. Het legt niet uit hoe een firewall werkt, maar hoe een CISO ervoor zorgt dat een organisatie haar informatierisico's werkelijk bestuurt: met een helder mandaat, eerlijke informatie aan het bestuur, goede relaties met de lijn, en zonder de rol van spelbreker.

Voor wie

- **Bestuurders en toezichthouders** die willen weten wat zij van een CISO mogen verwachten, en wat de CISO van hen nodig heeft.
- **Aankomende CISO's en securitymanagers** die willen weten wat de rol vraagt en of zij er klaar voor zijn.
- **Zittende CISO's** die hun positie, mandaat en effectiviteit willen versterken.

De aanbevolen leesroutes per doelgroep staan in het schrijfkader.

Opbouw

Deel I beschrijft de rol, de taken en de vaardigheden. Deel II gaat over governance: verwachtingen, positie, mandaat, organisatie, afbakening en beloning. Deel III behandelt relaties, invloed en perceptie, inclusief veelgemaakte fouten en netwerken. Deel IV bevat de toolkit en vier 90-dagenplannen. Vier bijlagen geven een begrippenlijst, een regelgevingsoverzicht, een overzicht van normen en de bronnen.

Elk hoofdstuk sluit af met een werkblok: samenvatting, reflectievragen, checklist, praktische opdrachten, template en do's en don'ts. Wie het boek als werkboek gebruikt, kan per hoofdstuk direct aan de slag.

Omgang met zekerheid

Aanbevelingen zijn waar nodig gelabeld als **Norm**, **Best practice**, **Context** of **Advies**. Wet- en regelgeving en beloningscijfers hebben een bron en peildatum. Waar openbare gegevens ontbreken, staat dat erbij en is een inschatting als zodanig gemarkeerd. Praktijkvoorbeelden zijn samengesteld uit herkenbare situaties; organisaties in voorbeelden zijn fictief, tenzij het om een openbare bron gaat.

Peildatum

De inhoud is bijgewerkt tot 5 oktober 2026. Regelgeving, normen en arbeidsmarktgegevens veranderen; bijlage D noemt wat bij een herdruk opnieuw moet worden gecontroleerd.

Hoofdstukindeling

Elk hoofdstuk beantwoordt één bestuurlijke of vakinhoudelijke hoofdvraag en levert minimaal één bruikbaar werkproduct op. De letter verwijst naar het inhoudelijk onderwerp uit de opdracht (A–N).

Nr.	Hoofdstuk	Hoofdvraag	Werkproduct(en)	Onderwerp
1	De CISO-rol: definitie en fundament	Wat is de CISO, en hoe verhoudt de rol zich tot verwante functies en de drie lijnen?	Rolafbakeningsmatrix, begrippenkaart RAMO	A
2	Wat een CISO doet	Welke taken vormen het vak, en hoe verschuift de nadruk met grootte en sector?	Takenkaart, tijdsbestedingsprofiel	B
3	Kerntaken in de praktijk I	Hoe voert een CISO governance, strategie, beleid, risico en advies concreet uit?	Governance-structuur, strategie op 1 pagina, risicomemo, adviesnota	B, J
4	Kerntaken in de praktijk II	Hoe organiseert een CISO cultuur, incidentrespons, keten, assurance, budget, metrics, architectuur en team?	Crisisdraaiboek-index, leveranciersbeoordeling, businesscase, dashboard, teamplan	B, J
5	Wat een CISO moet kunnen	Welke competenties maken het verschil, naast technische kennis?	Competentieprofiel, ontwikkelplan	C
6	Verwachtingen van bestuur en	Wat mag het bestuur	Verwachtingenmatrix,	D

Nr.	Hoofdstuk	Hoofdvraag	Werkproduct(en)	Onderwerp
	directie	redelijkerwijs verwachten, en wat niet?	rapportagekalender	
7	Positionering in de governance	Waar hoort de CISO in de organisatie, en waarom?	Modellenvergelijking, positioneringsadvies	E
8	Mandaat en onafhankelijkheid	Welke rechten heeft een CISO nodig om verantwoording te kunnen dragen?	Voorbeeld-mandaattekst, mandaattoets	G
9	Organisatie en span of control	Wie stuurt de CISO aan, direct en functioneel, per bedrijfsgrootte?	Organogrammen, RACI, formatierichtlijn	F
10	Taken die niet bij de CISO horen	Welke taken ondermijnen onafhankelijkheid of effectiviteit?	Afbakeningslijst met overgangsafspraken	I
11	Beloning	Wat verdient een CISO, en welke factoren bepalen dat?	Beloningsindicatie NL/BE, onderhandelingschecklist	H
12	De CISO en zijn stakeholders	Hoe werkt de CISO samen met CIO, CFO, GC, HR, audit, risk, compliance, FG en business?	Raakvlakken-RACI, relatieplan	Eis 9
13	Relatie met het bestuur	Wat mag een CISO van het bestuur vragen?	Bestuurscontract	K
14	Profilering en perceptie	Hoe wordt de CISO partner in	Gesprekksscripts, “ja, mits”-format	L

Nr.	Hoofdstuk	Hoofdvraag	Werkproduct(en)	Onderwerp
		plaats van rem?		
15	Fouten en anti-patronen	Welke patronen maken een CISO ineffectief?	Anti-patronencheck	Eis 8
16	Vakverenigingen en netwerken	Waar ontwikkelt en verbindt een CISO zich in NL en BE?	Netwerkoverzicht	M
17	Werkboektoolkit	Welke instrumenten heeft de CISO direct nodig?	Alle templates en checklists uit onderwerp N	N
18	Vier 90-dagenplannen	Hoe start een CISO in vier typische situaties?	4 × 90-dagenplan	Eis 10

Vast werkblok per hoofdstuk: samenvatting · reflectievragen · checklist(s) · praktische opdrachten · template of voorbeeldformat · do's en don'ts · voorbeelden voor klein, middelgroot en groot.

Schrijfkader

Dit kader legt vast voor wie het boek is, hoe het spreekt en hoe het met zekerheid omgaat. Het geldt voor alle hoofdstukken.

Doelgroep en leesroutes

Lezer	Wat de lezer zoekt	Aanbevolen route
Bestuurder (RvB, directie)	Wat verwacht ik, wat geef ik, hoe stuur ik?	H1, 6, 7, 8, 13, 17.2
Toezichthouder (RvC, RvT)	Hoe toets ik of security goed belegd is?	H1, 6, 7, 8, 15, 17.2
Aankomende CISO	Ben ik klaar, wat komt op me af?	H1–5, 17.1, 18.1
Zittende CISO	Hoe word ik effectiever en beter gepositioneerd?	H3–4, 8, 12–15, 17
Securitymanager	Hoe groei ik naar de CISO-rol?	H2–5, 9, 17.1

Toon en stijl

- Zakelijk, direct en toegankelijk. Korte zinnen, actieve vorm, concrete werkwoorden.
- Geen marketingtaal (“game changer”, “best-in-class”) en geen leeg jargon (“synergie”, “holistisch”).
- “De CISO” als vaste aanduiding; geen genderspecifiek voornaamwoord tenzij een praktijkvoorbeeld een persoon beschrijft.
- “Bestuur” = hoogste uitvoerende orgaan (RvB, directie, college). “Toezicht” = RvC, RvT of auditcommissie.
- Engelse vaktermen alleen waar die in Nederland en België gangbaar zijn (CISO, SOC, KPI, RACI); bij eerste gebruik kort gedefinieerd.

Labels voor zekerheid en normativiteit

Elke aanbeveling krijgt waar nodig een van vier labels, zodat de lezer weet hoe hard een uitspraak is.

Label	Betekenis	Voorbeeld
Norm	Volgt uit wet, regelgeving of een algemeen aanvaarde standaard	Onder NIS2 keurt het bestuur de risicobeheersmaatregelen goed en houdt er toezicht op
Best practice	Brede vakconsensus, maar niet verplicht	De CISO heeft een directe escalatielijn naar het bestuur
Context	Juiste keuze hangt af van grootte, sector of volwassenheid	CISO onder de CIO kan werken in een kleine, IT-gedreven organisatie
Advies	Mening van de auteur, onderbouwd	Leg het mandaat schriftelijk vast vóór de eerste werkdag

Organisatiegrootte en sectoren

Voorbeelden worden steeds uitgewerkt voor drie tot vier groottes. De indeling volgt grofweg de EU-mkb-definitie; voor security telt naast omvang ook complexiteit en regeldruk.

Categorie	Medewerkers (indicatief)	Typische CISO-invulling
Klein	10–49	Gedeelde of virtuele CISO, enkele dagen per maand
Middelgroot	50–249	Parttime of fulltime CISO, 0–2 fte eigen team
Groot	250–5.000	Fulltime CISO, eigen team en functionele lijn naar IT
Multinational of sterk	> 5.000 of onder intensief	CISO met afdeling, regionale of

Categorie	Medewerkers (indicatief)	Typische CISO-invulling
gereguleerd	toezicht	divisie-CISO's

Sectoren met eigen accenten: **overheid** (BIO2, politiek-bestuurlijke verantwoording), **zorg** (NEN 7510, patiëntveiligheid, beschikbaarheid), **finance** (DORA, toezicht DNB/NBB en AFM/FSMA), **industrie** (OT-security, safety, ketens) en **commercieel/tech** (snelheid, productsecurity, klanteisen).

Wettelijk kader: NIS2 in Nederland en België

NIS2 (Richtlijn (EU) 2022/2555) maakt cybersecurity uitdrukkelijk een bestuursverantwoordelijkheid. Dat raakt de kern van dit boek: het bestuur is eindverantwoordelijk, de CISO maakt die verantwoordelijkheid uitvoerbaar.

Land	Wet	Status	Toezicht en kader
Nederland	Cyberbeveiligingswet (Cbw), Stb. 2026, 187; uitgewerkt in het Cyberbeveiligingsbesluit (Stb. 2026, 189)	In werking sinds 15 augustus 2026; vervangt de Wbni	Sectorale toezichthouders; registratie-, zorg- en meldplicht; bestuurders moeten kennis en vaardigheden hebben om cyberrisico's te beoordelen
België	NIS2-wet van 26 april 2024	In werking sinds 18 oktober 2024	Centrum voor Cybersecurity België (CCB); CyberFundamentals (CyFun) als referentiekader

De Cbw raakt in Nederland ruim 8.000 organisaties. Sectorspecifieke regels (DORA voor finance, BIO2 voor overheid, NEN 7510 voor zorg) gaan voor of vullen aan; het boek benoemt dat per hoofdstuk.

Bronnen: Cyberbeveiligingsbesluit, Stb. 2026, 189 (NJB) (https://www.njb.nl/wetgeving/staatsbladen/cyberbeveiligingsbesluit/) · Accountancy Vanmorgen, 08-07-2026 (https://www.accountancyvanmorgen.nl/2026/07/08/cyberbeveiligingswet-en-wet-weerbaarheid-kritieke-entiteiten-scheppen-nieuwe-verplichtingen/). Belgische gegevens: algemene stabiele kennis, te controleren op ccb.belgium.be vóór publicatie.

Bron- en actualiteitsbeleid

- Wet- en regelgeving, beloningscijfers en verenigingsgegevens worden bij elk hoofdstuk voorzien van bron en peildatum.
- Beloningscijfers zijn **marktindicaties**: altijd een bandbreedte, nooit een puntwaarde, met de factoren die de spreiding verklaren.

- Praktijkvoorbeelden zijn samengesteld uit herkenbare situaties; namen en organisaties zijn fictief.
- Waar praktijk per land of sector verschilt, staat dat er expliciet bij. Geen absolute claims zonder label **Norm**.

Doorlopende thema's

Deze acht thema's komen in elk hoofdstuk terug waar ze relevant zijn: governance en onafhankelijkheid · spanning tussen advies en controle · de drie lijnen · NIS2 · mkb versus enterprise · politieke sensitiviteit · soft skills naast techniek · grenzen van maakbaarheid en verantwoordelijkheid.

Hoofdstuk 1 — De CISO-rol: definitie en fundament

De CISO is de functionaris die namens het bestuur zorgt dat informatiebeveiliging bestuurbaar is: risico's zichtbaar, keuzes expliciet, maatregelen belegd en effectiviteit aantoonbaar. De CISO is daarmee niet de eigenaar van alle beveiliging, maar wel van de vraag of de organisatie haar beveiliging goed bestuurt.

1.1 Wat een CISO is — en wat niet

Werkdefinitie (Advies). De Chief Information Security Officer is de hoogste functionaris voor informatiebeveiliging, die het bestuur adviseert over informatierisico's, het beveiligingskader vaststelt en bewaakt, de uitvoering daarvan door de lijn coördineert en toetst, en onafhankelijk rapporteert over de stand van beveiliging en restrisico.

Vier elementen uit die definitie bepalen de rest van dit boek:

1. **Namens het bestuur.** De CISO ontleent gezag aan het bestuur, niet aan IT. Zonder die verankering is de rol een titel zonder werking.
2. **Kader stellen en bewaken.** De CISO bepaalt wát goed genoeg is; de lijn bepaalt hoe en voert uit.
3. **Coördineren en toetsen.** De CISO stuurt vaak functioneel, niet hiërarchisch. Invloed is het belangrijkste instrument.
4. **Onafhankelijk rapporteren.** De CISO moet ongemakkelijk nieuws kunnen brengen zonder dat de eigen lijnmanager dat kan tegenhouden.

Wat een CISO níet is (Best practice):

- Niet de hoogste systeembeheerder of de "firewallbaas".
- Niet de persoon die elk risico persoonlijk accepteert. Risicoacceptatie ligt bij de eigenaar van het proces of systeem.
- Niet de interne auditor. De CISO toetst om te sturen; audit toetst onafhankelijk van sturing.
- Niet de garantie dat er geen incidenten komen. Volledige preventie bestaat niet; zie de grenzen van maakbaarheid in 1.6.

De titel versus de rol. In de praktijk dragen mensen met sterk uiteenlopende taken de titel CISO. Een "CISO" bij een mkb-bedrijf van 60 medewerkers die ook de firewall beheert, doet feitelijk iets anders dan een CISO bij een bank met 80 man personeel. Dit boek beoordeelt daarom de **rol** (wat iemand doet en mag), niet de titel.

1.2 Strategisch, tactisch en operationeel

De CISO-rol beweegt op drie niveaus. De verdeling verschuift met de grootte van de organisatie, maar een CISO die structureel meer dan de helft van de tijd operationeel bezig is, vervult in feite een andere rol.

Niveau	Kernvraag	Typische activiteiten	Output	Tijdsbesteding klein / middel / groot (indicatief)
Strategisch	Welke risico's accepteren we, en waar investeren we?	Strategie, risicobereidheid, bestuursadvies, positionering, toezichthouders	Securitystrategie, board-rapportage, risicobereidheidsverklaring	20% / 35% / 50%
Tactisch	Hoe vertalen we strategie naar programma's en kaders?	Beleid, normenkader, roadmap, budget, metrics, leveranciersbeleid, architectuurprincipes	Beleid, roadmap, KPI/KRI-set, jaarplan	35% / 40% / 35%
Operationeel	Werkt het, en wat gebeurt er nu?	Incidentcoördinatie, risicobeoordelingen, reviews, advies aan projecten, awareness-uitvoering	Incidentrapport, risicoanalyse, advies, testresultaten	45% / 25% / 15%

Context. In een klein bedrijf is operationeel werk onvermijdelijk. Dat is acceptabel zolang de CISO het strategische deel bewust reserveert en het bestuur weet dat operationele betrokkenheid de onafhankelijkheid beperkt.

Praktijkvoorbeelden

- *Klein (35 medewerkers, accountantskantoor).* Een virtuele CISO werkt vier dagen per maand. Eén dag per kwartaal is gereserveerd voor directieoverleg en risicobereidheid; de rest gaat naar MFA-uitrol, leveranciersvragen en een phishingoefening.
- *Middelgroot (180 medewerkers, logistiek).* De CISO zit wekelijks in het IT-overleg (tactisch), maandelijks bij de directie (strategisch), en neemt bij incidenten tijdelijk de coördinatie (operationeel), waarna een externe SOC-partner het overneemt.

- *Groot (3.000 medewerkers, gemeente).* De CISO laat operationeel werk over aan een securitymanager en SOC, en besteedt de helft van de tijd aan bestuur, college, gemeentesecretaris, ketenpartners en de BIO2-verantwoording.

1.3 De CISO naast verwante functies

Verwarring tussen rollen is de meest voorkomende oorzaak van “verantwoordelijk zonder macht”. De tabel geeft de typische afbakening (**Best practice**; titels en invulling verschillen per organisatie).

Functie	Kernverantwoordelijkheid	Lijn (drie lijnen)	Verhouding tot de CISO
CISO	Bestuurbaarheid van informatiebeveiliging: kader, advies, toetsing, rapportage	2e lijn (soms hybride)	—
Securitymanager	Uitvoering van het securityprogramma en operationele securitytaken	1e lijn of 2e lijn, afhankelijk van inrichting	Vaak ondergeschikt aan of rechterhand van de CISO
SOC-manager	Detectie, monitoring en eerste respons	1e lijn	Operationeel; levert data voor KPI’s en incidentinformatie
IT-manager	Beschikbaarheid en beheer van IT-diensten, inclusief technische maatregelen	1e lijn	Eigenaar van veel maatregelen die de CISO toetst
CIO	Informatievoorziening en IT-strategie	1e lijn (bestuurlijk)	Belangrijkste partner; mogelijk belangenconflict bij hiërarchische lijn
Risk manager / CRO	Integraal risicomanagement over alle risicotypen	2e lijn	Kaderstellend over methodiek; CISO levert informatierisico in
Compliance officer	Naleving van wet- en regelgeving en interne regels	2e lijn	Overlap bij NIS2, DORA, AVG; afspraken nodig
FG / DPO	Toezicht op naleving AVG, wettelijk onafhankelijk	2e lijn (wettelijk gepositioneerd)	Nauwe samenwerking; FG mag niet ondergeschikt zijn aan wie de verwerking

Functie	Kernverantwoordelijkheid	Lijn (drie lijnen)	Verhouding tot de CISO
			bepaalt
Internal Audit	Onafhankelijke toetsing van opzet, bestaan en werking	3e lijn	Toetst ook de CISO-functie zelf

Sectorverschillen

- **Finance (Norm/Best practice):** toezichthouders verwachten doorgaans een duidelijk tweedelijns-informatiebeveiligingsfunctie, gescheiden van IT. DORA versterkt die verwachting.
- **Overheid:** de CISO werkt vaak naast een CIO of informatiemanager; de BIO2 vraagt om een belegde verantwoordelijke en verantwoording richting bestuur en gemeenteraad of Staten.
- **Zorg:** NEN 7510 vraagt om aantoonbaar belegde verantwoordelijkheid. Vaak combineert men CISO en Privacy Officer in kleinere instellingen, met het risico van te brede verantwoordelijkheid (zie H10).
- **Industrie:** OT-security zit vaak bij engineering of operations. De CISO moet daar functionele zeggenschap over het kader krijgen, zonder safety-verantwoordelijkheid over te nemen.
- **Commercieel/tech:** productsecurity zit vaak bij de CTO; de CISO stelt het kader en toetst.

1.4 Verantwoordelijkheid, accountability, mandaat en eigenaarschap

Vier begrippen worden vaak door elkaar gebruikt. Wie ze niet scheidt, krijgt een CISO die overal op aangesproken wordt en nergens over beslist.

Begrip	Definitie	Vraag die het beantwoordt	Voorbeeld
Verantwoordelijkheid (responsibility)	De plicht om een taak uit te voeren	Wie doet het?	IT-beheer patcht de servers
Accountability (eindverantwoordelijkheid, rekenschap)	De plicht om verantwoording af te leggen over het resultaat, ook als anderen uitvoeren	Wie wordt erop aangesproken?	De CIO legt verantwoording af over de patchachterstand
Mandaat	De formele bevoegdheid om te beslissen, op te dragen of te escaleren	Wie mag het besluiten?	De CISO mag een systeem zonder MFA van internet laten afkoppelen bij acuut risico
Eigenaarschap	De rol die over een asset, proces of risico beslist en de gevolgen	Van wie is het?	De directeur Zorg is eigenaar van het EPD-risico en accepteert

Begrip	Definitie	Vraag die het beantwoordt	Voorbeeld
	draagt		restrisico

Kernregel (Best practice). Accountability vraagt om mandaat. Iemand verantwoordelijk houden voor een uitkomst waarover hij niets mag beslissen, is geen governance maar risico-afschuiving.

Hoe het meestal goed belegd is

- Het **bestuur** is eindverantwoordelijk voor informatiebeveiliging als geheel (**Norm** onder NIS2 voor entiteiten in scope).
- **Proces- en systeemeigenaren** zijn eigenaar van hun risico's en accepteren restrisico binnen de risicobereidheid.
- **IT en andere uitvoerders** zijn verantwoordelijk voor het implementeren en onderhouden van maatregelen.
- De **CISO** is accountable voor de kwaliteit van het kader, de juistheid en tijdigheid van risico-informatie, en het tijdig escaleren. De CISO is níet accountable voor het ontbreken van incidenten.

Voorbeeld van verkeerd belegd. Na een ransomware-incident vraagt de raad van toezicht waarom "de CISO dit niet heeft voorkomen". Uit de stukken blijkt dat de CISO de verouderde VPN-omgeving drie keer als hoog risico heeft gemeld, dat vervanging twee keer is doorgeschoven en dat niemand het risico formeel heeft geaccepteerd. De fout zit in de governance, niet bij de CISO. De les: leg risicoacceptatie altijd vast bij een eigenaar, met naam en datum.

1.5 De drie lijnen en de spanning tussen advies en controle

Het drielijnenmodel (IIA, herzien in 2020 als "Three Lines Model") onderscheidt uitvoering, ondersteuning en toezicht, en onafhankelijke toetsing.

Lijn	Rol	Wie (security-context)	Typische CISO-relatie
1e lijn	Bezit en beheerst risico's in de dagelijkse operatie	Business, IT, OT, development, leveranciersmanagement	De CISO adviseert, ondersteunt en stelt eisen
2e lijn	Stelt kaders, ondersteunt, monitort en daagt uit	CISO, risk management, compliance, FG	Positie van de CISO in de meeste volwassen modellen
3e lijn	Toetst onafhankelijk de opzet en werking van 1e en 2e lijn	Internal Audit, externe audit	Toetst ook de CISO-functie

Waar de CISO staat. In volwassen en gereguleerde organisaties staat de CISO in de 2e lijn (**Best practice**; in finance vaak **Norm** in de toezichtpraktijk). In kleinere organisaties is de CISO vaak hybride: hij geeft

advies, stelt kaders en voert ook uit. Dat is werkbaar als het bestuur weet waar de onafhankelijkheid ophoudt.

De spanning tussen advies en controle. De CISO moet tegelijk partner en toetser zijn. Dat is geen ontwerpfout, maar het vraagt bewust schakelen.

Aspect	Adviesrol	Controlerol
Doel	Helpen een goede keuze te maken	Vaststellen of de keuze en uitvoering voldoen
Houding	Meedenkend, oplossingsgericht	Onafhankelijk, kritisch, feitelijk
Moment	Vooraf en tijdens	Achteraf en periodiek
Risico bij overdrijven	Meeschrijven met de oplossing, daarna eigen werk toetsen	Gezien worden als politieagent, buitengesloten worden

Werkwijze om de spanning te hanteren (Advies)

1. Maak per traject expliciet in welke rol je zit: “Ik denk nu mee als adviseur; in Q3 toets ik de werking.”
2. Ontwerp geen oplossingen die je later zelf moet goedkeuren. Geef eisen en criteria, laat de lijn het ontwerp maken.
3. Laat de werking van kritieke maatregelen ook toetsen door de 3e lijn of een externe partij, zeker waar je zelf heeft meegeadviseerd.
4. Leg risicoacceptatie altijd bij de eigenaar; de CISO adviseert over acceptatie maar tekent niet.

Praktijkvoorbeelden

- *Middelgroot (zorginstelling, 900 medewerkers).* De CISO adviseert bij de aanbesteding van een nieuw roostersysteem en levert een eisenset. Bij oplevering vraagt de CISO een externe pentest in plaats van zelf te testen, omdat hij nauw betrokken was bij het ontwerp.
- *Groot (verzekeraar).* De 1e lijn heeft een eigen “Business ISO” per divisie; de CISO in de 2e lijn stelt het kader en toetst steekproefsgewijs. Internal Audit toetst jaarlijks het ISMS inclusief de CISO-functie.
- *Klein (softwarebedrijf, 40 medewerkers).* De CTO is ook CISO. Het bestuur laat jaarlijks een externe partij een review doen, zodat er alsnog een onafhankelijke blik is.

1.6 NIS2 als bestuurlijk kader en de grenzen van maakbaarheid

NIS2 legt de eindverantwoordelijkheid nadrukkelijk bij het bestuur. Voor entiteiten in scope moet het bestuur de risicobeheersmaatregelen goedkeuren, toezien op de uitvoering en over voldoende kennis beschikken; bestuurders kunnen worden aangesproken (**Norm**). In Nederland geldt dit via de Cyberbeveiligingswet sinds 15 augustus 2026, in België via de NIS2-wet sinds 18 oktober 2024.

Voor de CISO betekent dit drie dingen:

1. **Het bestuur heeft een eigen belang bij een goede CISO.** De CISO is het instrument waarmee bestuurders hun wettelijke plicht invullen. Dat is een sterk argument voor mandaat en toegang.
2. **De CISO kan de bestuursverantwoordelijkheid niet overnemen.** Het bestuur kan delegeren, maar niet de eindverantwoordelijkheid afschuiven. Een CISO-charter mag dat ook niet suggereren.
3. **Bestuurlijke kennis is een CISO-taak.** De CISO organiseert bestuurstraining en zorgt dat stukken het bestuur in staat stellen echt te beoordelen, niet alleen te tekenen.

Grenzen van maakbaarheid (Advies). Een CISO kan wel garanderen: een helder kader, eerlijke risico-informatie, tijdige escalatie en een voorbereide organisatie. Een CISO kan niet garanderen: dat er geen incident komt, dat leveranciers foutloos werken, of dat budgetkeuzes van anderen goed uitpakken. Wie dat onderscheid niet maakt, maakt de CISO tot zondebok en het bestuur tot schijnbaar gerustgesteld.

Werkblok hoofdstuk 1

Samenvatting

- De CISO maakt informatiebeveiliging bestuurbaar namens het bestuur; de rol is kaderstellend, adviserend, coördinerend en toetsend.
- De verhouding strategisch-tactisch-operationeel verschuift met de omvang; een structureel operationele CISO vervult feitelijk een andere rol.
- Scheid verantwoordelijkheid, accountability, mandaat en eigenaarschap; accountability zonder mandaat is onwerkbaar.
- De CISO staat bij voorkeur in de 2e lijn; in kleine organisaties is een hybride rol werkbaar mits bewust en transparant.
- NIS2 maakt het bestuur eindverantwoordelijk; de CISO maakt die verantwoordelijkheid uitvoerbaar maar kan haar niet overnemen.

Reflectievragen

1. Als je je eigen rol in één zin moet beschrijven, is dat dan een titel of een opdracht van het bestuur?
2. Welk percentage van je tijd ging de afgelopen maand naar operationeel werk, en heeft het bestuur daarvoor gekozen?
3. Van welke drie grootste risico's weet je precies wie de eigenaar is en wanneer het restrisico is geaccepteerd?
4. In welk lopend traject zit je tegelijk in de advies- en de controlerol, en hoe borg je dat?
5. Wat zou het bestuur na een groot incident van jou verwachten dat je had gedaan, en is dat vastgelegd?

Checklist: is de rol helder belegd?

- ☐ Er is een schriftelijke rolbeschrijving of CISO-charter, vastgesteld door het bestuur
- ☐ De CISO heeft een directe rapportage- of escalatielijn naar het bestuur
- ☐ Risico-eigenaarschap is per kritiek proces of systeem belegd, met naam
- ☐ Risicoacceptatie wordt schriftelijk vastgelegd door de eigenaar, niet door de CISO
- ☐ De afbakening met CIO, risk, compliance, FG en audit is vastgelegd

- ☐ Het bestuur weet of de CISO in de 2e lijn of hybride werkt, en wat dat betekent
- ☐ De werking van maatregelen wordt (ook) door een onafhankelijke partij getoetst
- ☐ Er is vastgesteld of de organisatie onder NIS2/Cbw valt en in welke categorie

Praktische opdrachten

1. **Tijdsanalyse (1 uur).** Deel je agenda van de laatste vier weken in naar strategisch, tactisch en operationeel. Vergelijk met de indicatie uit 1.2 en bespreek het verschil met je leidinggevende.
2. **Rolafbakening (2 uur).** Vul de matrix hieronder in voor je eigen organisatie en leg hem voor aan CIO, risk manager en FG.
3. **Eigenaarschapsscan (halve dag).** Neem de tien grootste informatierisico's. Noteer per risico eigenaar, laatste acceptatiedatum en wie het uitvoert. Elke lege cel is een governance-actiepunt.
4. **Bestuurstoets NIS2 (1 uur).** Formuleer drie vragen die het bestuur moet kunnen beantwoorden om aan de bestuursplicht te voldoen, en toets of de huidige rapportage die antwoorden geeft.

Template: rolafbakeningsmatrix

Onderwerp	CISO	CIO / IT	Risk	Compliance	FG / DPO	Internal Audit	Business-eigenaar
Informatiebeveiligingsbeleid vaststellen	Stelt op	Consulted	Consulted	Consulted	Consulted	Informed	Bestuur stelt vast
Risicomethodiek	Past toe voor IB	Informed	Stelt kader	Consulted	Consulted	Informed	Informed
Risicoacceptatie	Adviseert	Consulted	Bewaakt kader	Informed	Consulted bij persoonsgegevens	Informed	Accepteert
Technische maatregelen implementeren	Stelt eisen, toetst	Voert uit	—	—	—	Toetst periodiek	Informed
Incidentmelding NIS2/Cbw	Coördineert inhoud	Levert gegevens	Informed	Toetst termijn en vorm	Consulted bij datalek	Informed	Bestuur informeren
Toetsing werking	Monitort	Levert	Informed	Consulted	—	Toetst onafhanke	Informed

Onderwerp	CISO	CIO / IT	Risk	Compliance	FG / DPO	Internal Audit	Business-eigenaar
ISMS		bewijs				lijk	

Pas namen en rollen aan je eigen organisatie aan; lege of dubbele "Accountable"-cellen zijn het gespreksonderwerp.

Do's en don'ts

Do	Don't
Leg rol, mandaat en escalatielijn schriftelijk vast	Accepteer een titel zonder bijbehorende rechten
Benoem expliciet of je adviseert of toetst	Ontwerp oplossingen die je later zelf moet goedkeuren
Laat risico's accepteren door de eigenaar	Teken zelf voor risicoacceptatie "omdat niemand anders het doet"
Maak het bestuur bewust van zijn NIS2-eindverantwoordelijkheid	Wek de indruk dat de CISO die verantwoordelijkheid overneemt
Reserveer bewust tijd voor strategisch werk	Laat operationele brandjes je hele agenda vullen
Benoem wat je wel en niet kunt garanderen	Beloof een incidentvrije organisatie

Voorbeelden per organisatiegrootte

Grootte	Typische invulling	Belangrijkste aandachtspunt
Klein	Virtuele of gedeelde CISO, of IT-manager/CTO met CISO-taken	Zorg voor een minimale onafhankelijke toets, bijvoorbeeld een jaarlijkse externe review
Middelgroot	Parttime of fulltime CISO, hybride 1e/2e lijn	Leg vast welke operationele taken tijdelijk zijn en wanneer ze naar IT gaan
Groot	Fulltime CISO in de 2e lijn met eigen team	Borg de functionele lijn naar 1e-lijnssecurity en de directe toegang tot bestuur
Multinational / gereguleerd	Groeps-CISO met divisie- of land-CISO's	Eenduidig kader, lokale ruimte, en heldere verhouding met toezichthouders per land

Hoofdstuk 2 — Wat een CISO doet: het takenlandschap

Het CISO-vak bestaat uit veertien kerntaken, gegroepeerd in vier clusters: sturen, beschermen, voorbereiden en organiseren. Geen CISO doet alle veertien even intensief; de kunst is bewust kiezen welke taken nu het meeste risico wegnemen, en dat met het bestuur afspreken.

2.1 Veertien kerntaken in één overzicht

De kolom “Rol CISO” geeft aan hoe de CISO zich tot de taak verhoudt (**Best practice**):

- **Eigenaar:** de CISO levert het resultaat en is erop aanspreekbaar.
- **Kaderstellend:** de CISO bepaalt eisen en methode; anderen voeren uit.
- **Coördinerend:** de CISO brengt partijen samen en bewaakt samenhang.
- **Adviserend:** de CISO levert inbreng; een ander besluit.

#	Kerntaak	Cluster	Doel	Rol CISO	Kernoutput	Belangrijkste stakeholders
1	Governance van informatiebeveiliging	Sturen	Rollen, besluitvorming en verantwoording zijn helder belegd	Eigenaar	Governance-structuur, CISO-charter, overlegstructuur	Bestuur, toezicht, CIO, risk
2	Securitystrategie	Sturen	Meerjarige richting die aansluit op bedrijfsdoelen en dreiging	Eigenaar	Strategie op 1 pagina, meerjarenplan	Bestuur, CIO, business
3	Beleid en normenkaders	Sturen	Eén samenhangend, werkbaar stelsel van eisen	Eigenaar	Beleid, normenkader, standaarden	Compliance, IT, juridisch, FG
4	Risicomanagement	Sturen	Informatierisico’s zijn bekend, geprioriteerd en belegd	Kaderstellend	Risicoregister, risicoanalyses, acceptaties	Risk, proceseigenaren, IT