Competentiekompas Chief Information Security Officer (CISO)

Gids voor verantwoordelijkheden en competenties van de expert informatieveiligheid

Dit competentiekompas geeft richting aan de ontwikkeling van de rol als CISO. Het maakt inzichtelijk welke competenties, vaardigheden en verantwoordelijkheden belangrijk zijn bij het goed vervullen van de rol, en hoe je je kunt ontwikkelen binnen of richting de rol.

Zorgorganisaties gebruiken verschillende benamingen voor experts op het gebied van informatieveiligheid, zoals bijvoorbeeld: ISO, Security Officer of CISO. Ook verschillen ze sterk in hoe deze rol is belegd. Omdat de expert informatieveiligheid die zich richt op vraagstukken op operationeel, tactisch en strategisch niveau van informatieveiligheid meestal een CISO is, gebruiken we in dit Competentiekompas de term CISO.

Dit kompas laat zien hoe andere informatieveiligheid professionals zich kunnen ontwikkelen richting het niveau van een CISO, en maakt zichtbaar dat informatieveiligheid een volwaardige professionele verantwoordelijkheid is.

Het kompas bestaat uit twee delen:

- **Profiel**. Een richtinggevend overzicht van competenties, vaardigheden en kennis die nodig zijn om de rol van CISO goed te vervullen. Geen functiebeschrijving, maar een praktisch hulpmiddel dat helpt bij ontwikkelgesprekken, werving, selectie en scholing.
- **Reflectie- en ontwikkelingsvragen**. Een hulpmiddel dat CISO's helpt om stil te staan bij hun groei, en bestuurders en HR ondersteunt bij gesprekken over verdere professionalisering en versterking van de rol.

Aan wie geeft dit kompas richting?

- **CISO's** (en andere informatieveiligheidsprofessionals die zich tot CISO willen ontwikkelen) gebruiken het kompas om te reflecteren op hun rol. Ze zetten het in tijdens jaargesprekken of intervisie om leerdoelen te bepalen en een persoonlijk ontwikkelplan te maken.
- **Bestuurders** gebruiken het kompas om gericht in gesprek te gaan over de positie, rol en ontwikkeling van de CISO.
- **HR-professionals** zetten het in bij het werven, selecteren en begeleiden van CISO's.

Waarom juist nu?

De rol van een CISO verandert snel. Cyberdreigingen nemen toe (Z-CERT), wet- en regelgeving wordt strenger met de ingang van de Cyberbeveiligingswet (NIS2) en de zorg wordt steeds afhankelijker van digitale systemen. Incidenten kunnen direct de continuïteit van zorg en patiëntveiligheid raken.

In gesprekken met deelnemers zien we dat de uitvoering van informatieveiligheid in veel zorgorganisaties nog versnipperd is. Er is niet altijd een formele CISO-rol belegd; taken liggen soms bij professionals die dit naast hun reguliere werk doen, zonder de tijd of positie om het thema structureel te borgen. Daarbij ziet IVGZ in de praktijk dat CISO's of professionals met CISO-taken vaak tegen grenzen aanlopen bij het versterken van informatieveilig gedrag. Draagvlak ontbreekt geregeld, en bestuurders en teams geven het onderwerp te weinig prioriteit. Een goed toegeruste CISO kan dit patroon doorbreken door informatieveiligheid te verbinden met de dagelijkse praktijk en strategische doelen.

Informatieveiligheid gaat over meer dan techniek: het raakt aan menselijk gedrag, werkprocessen en bestuurlijke keuzes. Om gegevens vertrouwelijk, integer en beschikbaar te houden, is samenwerking tussen al deze onderdelen cruciaal. De CISO speelt hierin een strategische rol, door richting te geven, risico's te duiden en bestuurders gevraagd en ongevraagd advies te geven om afgewogen keuzes te maken. Dat vraagt om strategisch inzicht, advieskracht, verander- en projectmanagementvaardigheden én sterke sociale competenties naast inhoudelijke kennis.

IVGZ ontwikkelt daarom een nieuw competentiekompas dat verder gaat dan een standaard profiel. Het schetst een compleet beeld van de meest senior informatieveiligheidsrol in de zorg, inclusief de ontwikkeling die nodig is om informatieveilig gedrag duurzaam te versterken.

Onderdeel 1: profiel CISO

Taken- en verantwoordelijkheden

Planvorming en beleid

De CISO…

- Ontwikkelt en implementeert beleid en kaders, afgestemd op de zorgcontext en geldende wet- en regelgeving (AVG, NIS2/CBW, NEN 7510).
- Evalueert en vernieuwt jaarplannen in lijn met meerjarenplannen, waarbij informatieveiligheid als integraal onderdeel van de bedrijfsvoering wordt meegenomen.
- Volgt externe ontwikkelingen (o.a. dreigingsbeeld Z-Cert) en vertaalt deze naar beleid en plannen voor de organisatie.
- Richt het ISMS in en zorgt voor het onderhoud ervan.

Coördineren

De CISO…

- Coördineert organisatiebrede projecten, jaarplannen en activiteiten op het gebied van informatieveiligheid.
- Coördineert en signaleert of de organisatie voldoet aan de norm voor informatiebeveiliging NEN 7510.
- Stemt af met betrokken afdelingen (IT, kwaliteit, HR, facilitair/compliance, zorgprofessionals) en borgt samenwerking.
- Vertegenwoordigt de organisatie extern bij grote incidenten, meldt deze bij externe instanties en zorgt voor afhandeling.
- Organiseert IB-assessments, tests, reviews en audits.

Uitvoeren

De CISO…

- Houdt toezicht op naleving van beleid en rapportages, inclusief audits en assessments.
- Ontwikkelt richtlijnen, standaarden en methodieken voor informatieveiligheid en borgt de naleving.
- Bewaakt budgetten en middelen voor informatieveiligheid.
- Heeft inzicht in het gedrag binnen de organisatie, analyseert dit en kiest en monitort passende interventies om bewustwording en veilig gedrag te versterken.
- Onderhoudt contact met externe organisaties zoals Z-CERT.
- Neemt deel aan CISO-netwerken.

Ondersteunen

De CISO…

- Is eerste aanspreekpunt voor bestuur en management bij informatieveiligheidsvraagstukken.
- Ondersteunt leidinggevenden en teams bij het versterken van bewustzijn en informatieveilig gedrag.
- Vertegenwoordigt de organisatie en treedt op als inhoudelijke expert bij auditors, toezichthouders, leveranciers en samenwerkingsverbanden.
- Wisselt kennis en ervaring uit in regionale en landelijke netwerken.

Adviseren

De CISO…

- Adviseert bestuur en management gevraagd en ongevraagd over strategische keuzes, beleid, incidenten op het gebied van informatieveiligheid.
- Adviseert bestuur en management gevraagd en ongevraagd over nieuwe ontwikkelingen en innovaties, zoals inzet van AI, veranderende wet- en regelgeving (CBW). Blijft op de hoogte van de laatste stand van de techniek en relevante ontwikkelingen.
- Adviseert het crisisteam bij cyberaanvallen of andere incidenten die continuïteit en patiëntveiligheid raken.

Rapporteren

De CISO…

- Rapporteert periodiek aan het bestuur en management over de status van informatieveiligheid, risico's, maatregelen en incidenten.
- Zorgt dat successen en verbeterpunten zichtbaar zijn in de organisatie.

Competenties[1]

- **Adviesvaardigheden**
  - Adviseert bestuur en management gevraagd en ongevraagd. Weet ingewikkelde risico's te vertalen naar een helder verhaal dat overtuigt. Brengt verschillende belangen samen en helpt om gedrag en cultuur blijvend te veranderen.
- **Strategisch inzicht**
  - Verbindt informatieveiligheid met strategische doelen en maatschappelijke ontwikkelingen zoals NIS2, AVG en toezicht. Vertaalt beleid naar praktische implementaties.
- **Risicomanagement**

[1] In kleinere zorgorganisaties, waar de CISO-rol vaak een nevenfunctie is, adviseren we te starten met drie competenties die de grootste impact hebben: risicomanagement, adviesvaardigheid en motiveren. Deze vormen de basis om draagvlak te creëren, samenwerking te versterken en bewustwording van informatieveiligheid op te bouwen.

    - Brengt risico's op het gebied van beveiligingsvraagstukken in kaart, prioriteert en vertaalt deze naar heldere en concrete adviezen voor bestuur en management.
- **Sociale vaardigheden**
    - Beschikt over luistervaardigheid, weet weerstand te overbruggen en creëert draagvlak.
- **Projectmanagement**
    - Initieert en begeleidt projecten en programma's op het gebied van informatieveiligheid. Bewaakt voortgang, budget en resultaten en adviseert bij andere trajecten.
- **Organisatiesensitiviteit**
    - Herkent uiteenlopende belangen en houdt rekening met werkdruk en zorgpraktijk. Oog voor deze verschillende belangen die gewogen moeten worden. Weegt zorgvuldig af en kiest haalbare oplossingen.
- **Motiveren**
    - Inspireert en stimuleert anderen om informatieveilig te werken, ook wanneer dit extra inzet vraagt in de dagelijkse praktijk. Maakt veilig gedrag zichtbaar en vanzelfsprekend en weet veranderingen blijvend te verankeren. Weet bestuur en management actief te betrekken en te overtuigen van het belang van beleid en uitvoering, ook wanneer het onderwerp minder urgent wordt ervaren.

Kennis en ervaring

Een CISO heeft:

- Afgeronde relevante HBO/universitaire opleiding of daarmee vergelijkbaar niveau van kennis en vaardigheden.
- Grondige kennis van informatiebeveiliging, door het behalen van een certificering op bijvoorbeeld:
    - Certified Information Security Manager (CISM) (pré);
    - Certified Information Systems Security Professional (CISSP);
- Kennis van:
    - NEN 7510 (Internationale standaard voor informatiebeveiliging);
    - CBW/NIS2 (Netwerk- en Informatiebeveiliging Richtlijn);
    - Basiskennis van de Algemene verordening gegevensbescherming (AVG).
- Technische kennis: de CISO begrijpt hoe technologie de bedrijfsdoelen van de organisatie ondersteunt en hoe beveiliging hiermee samenhangt. Daarnaast heeft hij/zij een goed begrip van de cloudomgeving en identiteitsbeheer (IAM).
- Ruime (ongeveer 5 jaar) praktijkervaring met informatie- en gegevensbeveiliging in complexe organisaties.
- Ervaring met gedragsverandering, omdat informatieveiligheid niet alleen techniek maar vooral ook mensen raakt.
- Ervaring in het aansturen van projecten en/of programma's op het gebied van informatieveiligheid.

Plaats in de organisatie

- De CISO heeft een onafhankelijke positie en rapporteert rechtstreeks aan de Raad van Bestuur.
- Vanuit die positie waakt de CISO over de informatieveiligheid van de organisatie, signaleert risico's vroegtijdig en brengt deze in bij het bestuur en management.
- De CISO staat dicht bij het bestuur en helpt om strategische keuzes te maken die patiëntveiligheid, zorgcontinuïteit en informatieveiligheid versterken.
- Hij/zij brengt bestuur, management en praktijk samen en zorgt dat informatieveiligheid een terugkerend thema is in het bestuurlijk gesprek.

Onderdeel 2: Reflectievragen en reflectieformulier competenties

Dit onderdeel ondersteunt CISO's bij hun professionele ontwikkeling en is bedoeld als instrument voor zelfevaluatie. De vragen helpen om systematisch te reflecteren op de eigen rol, de samenwerking met bestuur en organisatie, en de manier waarop informatieveiligheid wordt ingebed in strategie en bedrijfsvoering. Hoewel de vragen zijn geformuleerd voor zelfreflectie door de CISO, kunnen ook bestuurders, leidinggevenden en HR-professionals ze gebruiken om vanuit hun eigen perspectief het gesprek aan te gaan met de CISO over diens rol, groei en ontwikkelbehoeften. Het uitgangspunt is een leven lang leren. Door regelmatig stil te staan bij het eigen handelen en ontwikkelbehoeften zichtbaar te maken, ontstaat inzicht in professionele groei en een basis voor een verdiepend gesprek over ontwikkeling in deze rol.

Reflectievragen

1. Rapporteren

- Hoe dragen mijn analyses en rapportages aantoonbaar bij aan het versterken van de digitale weerbaarheid van de organisatie?
- Begrijpt het bestuur de risico's, keuzes en prioriteiten die ik presenteer, en hoe toets ik of mijn boodschap goed landt?
- Hoe maak ik de resultaten van informatieveiligheid (successen, knelpunten, trends) zichtbaar en bestuurlijk relevant?

2. Adviseren

- Hoe ondersteun ik bestuur en management bij strategische keuzes door verschillende adviesstijlen in te zetten, van meedenken tot uitdagen?
- In welke mate breng ik informatieveiligheid in verband met kwaliteit van zorg, patiëntveiligheid en organisatiedoelen?
- Hoe gebruik ik gedragsinzichten om bestuurders en leidinggevenden te helpen beter geïnformeerde beslissingen te nemen?

3. Coördineren

- Hoe zorg ik dat alle betrokken afdelingen (IT, kwaliteit, HR, facilitair/compliance, zorgprofessionals) hun rol in informatieveiligheid kennen en uitvoeren?
- Hoe bevorder ik samenwerking tussen deze disciplines zodat informatieveiligheid een gedeelde verantwoordelijkheid wordt?
- Waar ontstaan nog knelpunten in samenwerking of afstemming, en wat is er nodig om die te verbeteren?

4. Ondersteunen

- Hoe breng ik samen met bestuurders en leidinggevenden het gesprek over veilig gedrag en organisatiecultuur structureel op gang?
- Hoe stimuleer ik medewerkers om verantwoordelijkheid te nemen voor veilig handelen, zonder dat dit als controle wordt ervaren?
- Hoe benut ik mijn rol als sparringpartner om bewustwording en eigenaarschap binnen teams te versterken?

5. Planvorming en beleid

- Hoe borg ik dat informatieveiligheid een vast onderdeel is van de jaar- en meerjarenplannen van de organisatie?
- Hoe vertaal ik externe ontwikkelingen (zoals NIS2/CBW, het dreigingsbeeld van Z-CERT of nieuwe technologieën) naar concreet beleid en prioriteiten?
- Hoe evalueer ik of beleid en maatregelen daadwerkelijk bijdragen aan patiëntveiligheid en continuïteit van zorg?
- Welke trends (bijvoorbeeld AI, CBW/NIS2, nieuwe wetgeving) beïnvloeden mijn rol de komende 12-24 maanden, en hoe vertaal ik deze naar beleid en plannen?

6. Uitvoeren

- Hoe houd ik toezicht op naleving zonder dat informatieveiligheid een papieren werkelijkheid wordt?
- Welke interventies zet ik in om bewustwording en gedrag duurzaam te beïnvloeden, en hoe meet ik het effect daarvan?
- Hoe gebruik ik mijn externe netwerk (zoals Z-CERT en CISO-netwerken) om actuele dreigingen en kennis te vertalen naar concrete acties binnen de organisatie?

Competentie	Reflectie	Doel/actie
Adviesvaardigheid		
Strategisch inzicht		
Risicomanagement		
Sociale vaardigheden		
Projectmanagement		
Organisatiesensitiviteit		
Motiveren		

	Ontwikkeldoelen voor de komende periode
1	
2	
3	
4	
5	

Colofon

In dit competentiekompas zijn inzichten van ervaringsdeskundigen uit de zorg verwerkt.

Het competentiekompas is een uitgave van het programma Informatieveilig gedrag in de zorg.

Het programma Informatieveilig gedrag in de zorg wordt uitgevoerd door stichting ECP | Platform voor de Informatiesamenleving in opdracht van het ministerie van VWS. De brancheorganisaties ActiZ, de Nederlandse ggz, NFU, NVZ en VGN zijn bij het programma betrokken.

Versie 1, november 2025 ©Informatieveilig gedrag in de zorg

Auteurs

Lourens Dijkstra de, IVGZ | Platform voor de Informatiesamenleving

Sietske Rozie, IVGZ | Platform voor de Informatiesamenleving

Mara van Heffen, IVGZ | Platform voor de Informatiesamenleving

Communicatie

Demi van Spronssen, ECP | Platform voor de Informatiesamenleving