Behorende bij het Informatieclassificatieraamwerk van de Vlaamse overheid

Vlaamse overheid

De rol van de CISO – Blauwdruk van het profiel

Versie: maart 2023

Bron: Team Informatieveiligheid

Doelgroep: Entiteiten die een security officer willen aanstellen

DIGITAAL VLAANDEREN

Voor een **veilige** digitale overheid

Een CISO vervult een organisatie-ondersteunende rol op strategisch of tactisch niveau

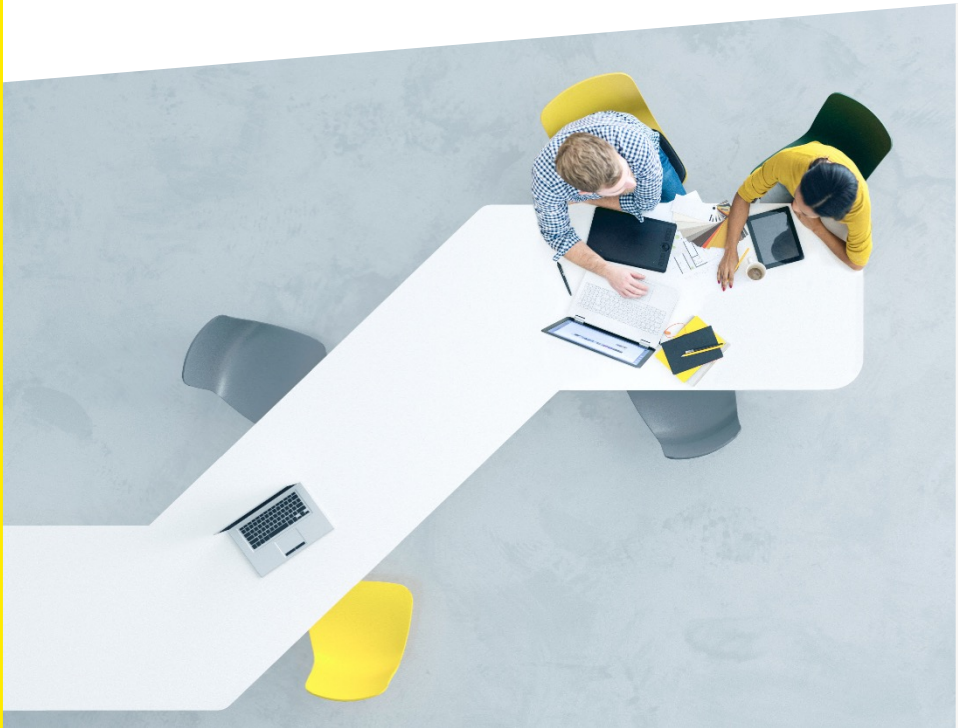
DIGITAAL VLAANDEREN

De Chief/Corporate Information Security Officer (CISO) is een beroepsprofiel dat vandaag de dag in veel organisaties terug te vinden is. Deze rol wordt dikwijls op verschillende manieren ingevuld met een wildgroei en verscheidenheid aan taken en verantwoordelijkheden, van strategisch tot operationeel. Deze handreiking geeft een blauwdruk van deze rol, holistisch gezien binnen de beroepsgroep van informatiebeveiligers en het cybersecurity skills framework van de Europese Unie.

Een CISO:

- *Definieert het informatiebeveiligingsbeleid en de informatieveiligheidsstrategie vanuit een op risico gebaseerde benadering. Hierbij houdt hij rekening met een continu veranderend dreigingsbeeld en analyseert daarbij trends en organisatiebehoeften.*
- *Richt de informatiebeveiligingsorganisatie in, definieert de daarvoor benodigde middelen en wijst ze toe.*
- *Initieert en coördineert de implementatie van informatiebeveiliging voor de hele organisatie, houdt toezicht vanuit een tweedelijnsrol en rapporteert aan het topkader.*
- *Zorgt voor een geschikt niveau van informatiebeveiliging en informatiebeveiligingsgedrag in de organisatie, gebaseerd op de behoeften en de risicobereidheid van de organisatie.*
- *Wordt door interne en externe belanghebbenden gezien als de deskundige op het gebied van informatiebeveiligingsstrategie.*

De aanstelling van een CISO binnen de entiteiten van de Vlaamse overheid is niet verplicht, maar aan te bevelen. Eventueel kan de rol gecombineerd worden met een andere organisatie-ondersteunende rol.



Raadpleeg het Informatieclassificatie raamwerk voor meer informatie **via deze QR:**

Profielbeschrijving CISO

DIGITAAL VLAANDEREN

Kerntaken

ORGANISATIE EN BELEID

- Definieert de informatiebeveiligingsstrategie en het informatiebeveiligingsbeleid
- Definieert richtlijnen, methodieken en een risicobeheerproces voor informatiebeveiliging
- Organiseert de benodigde informatiebeveiligingsexpertise
- Initieert organisatie-brede informatiebeveiligingsactiviteiten en -projecten
- Levert praktische ondersteuning bij de uitvoering van strategie en beleid
- Stemt af met andere veiligheidsdomeinen, waaronder fysieke beveiliging, gegevensbescherming, en risico- en continuïteitsmanagement
- Zet een calamiteitenorganisatie op en coördineert de reactie op ernstige informatiebeveiligingsincidenten

CONTROLE EN EVALUATIE

- Borgt en monitort:
  - De uitvoering van de informatiebeveiligingsstrategie en het informatiebeveiligingsbeleid
  - Informatiebeveiligingsbewustzijn binnen de organisatie
  - De kwaliteit van informatieklassebepalingen en -risicoanalyses
  - De effectiviteit van beheersmaatregelen
  - Relevante (opkomende) organisatie-brede risico's en adequate response
  - Compliance met relevante wet- en regelgeving
  - De naleving van het beleid d.m.v. reviews en tweedelijns audits
- Informeert het topkader over de status van informatiebeveiliging, het algehele risicoprofiel en presenteert verbetervoorstellen

Competenties

VAKGEBIED

- ✓ Strategieontwikkeling
- ✓ Informatiebeveiligingsbeheer
- ✓ Risicobeheer
- ✓ Audit

ALGEMEEN

- ✓ Leiderschap
- ✓ Relatiebeheer
- ✓ Communicatie
- ✓ Overtuigingskracht
- ✓ Organisatiesensitiviteit
- ✓ Management
- ✓ Analytisch vermogen
- ✓ Integriteit

Achtergrond

ERVARING

- ✓ Ruime werkervaring in een informatiebeveiligingsberoep
- ✓ Ruime werkervaring in een managementfunctie
- ✓ Relevante wet- en regelgeving kennis

OPLEIDING

- ✓ Afgeronde relevante Master-opleiding of vergelijkbaar niveau van kennis en vaardigheden
- ✓ Aanvullende relevante beroepscertificeringen

**Indicatief voor een (middel)grote entiteit, pas het profiel aan op uw organisatie*

Veelvoorkomende misvattingen

DIGITAAL VLAANDEREN

Taak van de CISO

Op organisatieniveau:

✓ **Informatieklassebepaling**
Definieert het proces, overziet klassebepalingen en bewaakt de kwaliteit

✓ **Informatierisicobeheer**
Definieert het proces, definieert criteria voor risicoappetijt, voert organisatie-brede risicoanalyses uit, overziet het risicolandschap, aggregeert risico's, adviseert en rapporteert aan het topkader

✓ **Beheersmaatregelen**
Definieert minimale beheersmaatregelen, levert richtlijnen en hulpmiddelen, monitort compliance en controleert en rapporteert over de effectiviteit van beheersmaatregelen

✓ **Incidentenbeheer**
Coördineert kritieke organisatie-brede beveiligingsincidenten en -calamiteiten en gebruikt de opgedane kennis om het beleid en de minimale maatregelen te verbeteren

✓ **Expertise**
Is een expert in strategie, beleid, managementraamwerken en -processen

Geen taak van de CISO

Op assetniveau:

× **Informatieklassebepaling**
Bepaalt de klasse van informatie voor alle individuele assets

× **Informatierisicobeheer**
Stelt de risicoappetijt vast, voert risicoanalyses uit op assetniveau en is eigenaar van de risico's

× **Beheersmaatregelen**
Selecteert, ontwikkelt, implementeert en/of opereert beheersmaatregelen

× **Incidentenbeheer**
Beheert alle informatiebeveiligingsincidenten

Voor bovenstaande taken is meestal de eigenaar van de asset (dienst, product, proces) verantwoordelijk en kan bij de uitvoering worden ondersteund door een security specialist

× **Expertise**
Is een expert in technologische architectuur en beveiligingsoplossingen

Deze expertise zit vaak bij een security architect of specialist

Toelichting

In de regel opereert de CISO op strategisch en tactisch niveau in een tweedelijnsrol en bestrijkt het domein van informatiebeheer in de breedste zin van het woord. Zijn rol is niet beperkt tot de ICT-voorzieningen.

Iedere organisatie is anders en het is niet ongebruikelijk dat de CISO operationele verantwoordelijkheden heeft. Dit is afhankelijk van de grootte van de organisatie, het maturiteitsniveau en de beschikbaarheid van gekwalificeerd personeel. Het mixen van verantwoordelijkheden vraagt enige waakzaamheid. Vanuit regelgeving en industrienormen wordt functiescheiding verwacht en vermijding van belangenvermenging. De CISO verantwoordelijk stellen voor zowel beleid als toezicht in combinatie met verantwoordelijkheid voor de operationele uitvoering zorgt niet voor de juiste resultaten.

Bepaalde mate van onafhankelijkheid is wenselijk om kritisch de implementatie van het beleid te kunnen toetsen. Eigenaarschap van risico's en beheersmaatregelen dient zo veel mogelijk in de lijn te worden belegd en geïntegreerd in bestaande processen.

Zie het Vo Informatieclassificatieraamwerk voor andere blauwdrukken van informatiebeveiligingsrollen.