TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Handreiking functieprofiel Chief Information Security Officer (CISO)

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Handreiking IB-functieprofiel Chief information security officer (CISO)’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Doel

Dit document biedt organisaties binnen de Rijksoverheid een handreiking bij het inrichten van de informatiebeveiligingsfunctie. Het beschrijft de functie en het profiel van een Chief Information Security Officer (CISO) en gaat in op de rol en de meerwaarde van een CISO in een organisatie binnen de Rijksoverheid. Ook rol van het lijnmanagement ten aanzien van informatiebeveiliging is beschreven. De uitgangspunten over de rol en het profiel van een CISO zijn afkomstig van de BIR.

Doelgroep

Dit document is van belang voor de directie en personeelszaken.

Reikwijdte

Dit document heeft voornamelijk betrekking op de maatregelen 6.1.2 en 8.1.1 van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Relatie met overige producten

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Informatiebeveiligingsbeleid
- PVIB beroepsprofielen informatiebeveiliging[1]

[1] http://www.pvib.nl/nieuws/17696378/16-05-2014/Whitepaper-Beroepsprofielen-Informatiebeveiliging-UPDATE-

Inhoudsopgave

1 Inleiding

Dit document geeft ondersteuning bij het inrichten van de Informatiebeveiligingsfunctie binnen een organisatie. Veel organisaties binnen de Rijksoverheid hebben de rol van beveiligingsfunctionaris benoemt voor de uitvoering van specifieke (wettelijke) verantwoordelijkheden, zoals die bijvoorbeeld voortvloeien uit de Wet bescherming persoonsgegevens (Wbp). Doordat informatieveiligheid een integrale verantwoordelijkheid van de directie betreft, hoort het generieke onderwerp informatiebeveiliging thuis binnen de bedrijfsvoering van een organisatie. Dit waarborgt integraliteit, eenheid en verantwoordelijkheid van de lijnorganisatie. Deze bredere invulling komt tot uiting in artikel 6.1.2.1 van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Voor de invulling van de informatiebeveiligingsfunctie binnen een organisatie spreekt de BIR van een Chief Information Security Officer (CISO). Afhankelijk van de grootte van de organisatie kan de informatiebeveiligingsfunctie uit één of meerdere personen bestaan. Bij veel organisaties (tot ong. 600 medewerkers) wordt de CISO-functie ook parttime ingevuld, bijvoorbeeld als combinatie van de CISO-rol met een verwante (staf)functie. Dat kan dan leiden tot een meer algemene functiebenaming (bijvoorbeeld beleidsmedewerker).Het inrichten van de informatiebeveiligingsfunctie laat onverlet dat informatieveiligheid een verantwoordelijkheid van iedere medewerker van een organisatie is.

1.1 Doelstelling

Het doel van deze handreiking is het bundelen en structureren van beschikbare informatie over de CISO-functie voor het vormgeven van deze functie in een organisatie met de BIR als uitgangspunt.

1.2 Doelgroep

Deze handreiking is ten eerste bestemd voor functionarissen binnen de organisatie die beslissen of, en in welke vorm er een CISO-functie komt. De directie neemt hierover een beslissing. Personeelszaken en management zullen een belangrijke adviserende en voorbereidende rol hebben.

Ten tweede vormt deze handreiking een hulpmiddel om te komen tot concrete invulling van de functie. Personeelszaken en management vinden in deze handreiking concrete beschrijvingen waarmee een gewenst functieprofiel kan worden samengesteld.

Ten derde vindt de beoogde of nieuw aangestelde CISO in deze handreiking aanknopingspunten om de functie in de praktijk vorm te geven.

1.3 Reikwijdte

Deze handreiking is bedoeld om te komen tot een functieprofiel voor een CISO. Een functieprofiel CISO is in zekere mate organisatiespecifiek. Het geformuleerde basisprofiel zal in veel organisaties toepasbaar zijn. Verder bevat deze handreiking aandachtspunten om de functie op gewenste punten aan te scherpen. Het opzetten van een profiel is op zichzelf een belangrijk proces, waardoor een organisatie scherp krijgt waar eigen behoefte ligt.

1.4 Werkwijze en leeswijzer

Voor dit document is gebruik gemaakt van de inzichten van het Platform voor Informatie Beveiligers (PvIB). Het PvIB kan gezien worden als de beroepsorganisatie van en voor CISO's en is brancheonafhankelijk. Binnen het PvIB is een whitepaper opgesteld over functies in de informatiebeveiliging. Daarnaast is voor dit document onder meer gebruik gemaakt van de maatregelen uit de Baseline Informatiebeveiliging Rijksdienst (BIR).

Dit document is opgebouwd uit de volgende hoofdstukken:

- In hoofdstuk 2 wordt een achtergrond geschetst bij het werk van een CISO;
- In hoofdstuk 3 wordt de meerwaarde van een CISO voor een organisatie beschreven;
- In hoofdstuk 4 wordt de basis gelegd voor een functieprofiel voor een CISO;
- Beschrijving van een basisfunctieprofiel opgesteld op basis van het voorgaande (bijlage 1).

2 Achtergrond informatiebeveiliging

Om digitale veiligheid te waarborgen worden in wet- en regelgeving in toenemende mate eisen betreffende informatiebeveiliging aan organisaties binnen de Rijksoverheid opgelegd.

Veel organisaties hebben informatiebeveiligingsbeleid opgesteld. Daarin wordt in hoofdlijnen beschreven hoe de organisatie van de informatiebeveiliging binnen een organisatie is ingericht. Vervolgens worden taken, verantwoordelijkheden en bevoegdheden met betrekking tot informatiebeveiliging vastgesteld en toegewezen aan betrokkenen. Binnen de Baseline Informatiebeveiliging Rijksdienst (BIR) betreft dat hoofdstuk 5 ‘Beveiligingsbeleid’ en hoofdstuk 6 ‘Beveiligingsorganisatie’.

Het aanstellen of benoemen van een verantwoordelijke functionaris is vaak de eerste stap na het opstellen van informatiebeveiligingsbeleid. Hiervoor kan onder meer gebruik worden gemaakt van het in dit document beschreven basisprofiel. De plaatsing in de organisatie is hierbij van belang, omdat dit in de praktijk lastig blijkt aan te passen. Verder kan de CISO, wanneer deze is aangesteld, als eerste taak krijgen om de informatiebeveiligingsorganisatie in kaart te brengen en een meer gedetailleerd functieprofiel op te stellen. Dit laatste moet wel in overeenstemming met het proceshandboek zijn en daarin ook verwerkt worden.

Ook in het geval de organisatie nog geen informatiebeveiligingsbeleid heeft, is het een goede eerste stap om een CISO aan te stellen. Wie kan het complete spectrum aan informatiebeveiliging immers beter overzien en coördineren dan een daarvoor speciaal aangestelde (op het vakgebied informatiebeveiliging deskundige) functionaris? Eén van zijn/haar eerste taken is dan het opstellen van het genoemde beleid. Hierbij moet worden opgemerkt dat de verantwoordelijkheid voor informatiebeveiliging ligt bij de directie. De CISO heeft een ondersteunende en adviserende rol.

Veel organisaties zullen een manager informatiebeveiliging aanstellen, die de algehele verantwoordelijkheid krijgt voor de ontwikkeling en implementatie van de beveiliging en ondersteuning verleent bij het vaststellen van de benodigde maatregelen. De verantwoordelijkheid voor het beschikbaar stellen van middelen en het implementeren van de maatregelen ligt echter vaak bij individuele managers. Het is van belang om voor elk informatiesysteem een ‘eigenaar’ aan te wijzen, die vervolgens verantwoordelijk is voor de dagelijkse beveiliging ervan.

De CISO heeft tevens een adviserende rol met betrekking tot crisis- en calamiteitenorganisatie wanneer er verwevenheid tussen de informatievoorziening en operationele techniek, zoals ICS/SCADA, bestaat. Beschikbaarheidsproblemen in de informatievoorziening kunnen in specifieke gevallen bijvoorbeeld leiden tot problemen met operationele techniek.

3 Wat is de meerwaarde van een CISO?

Organisaties doen ook zonder dat er een CISO is aangesteld meestal al veel op het gebied van informatiebeveiliging. Binnen die bestaande activiteiten zijn er verschillende rollen te onderkennen: het lijnmanagement is eindverantwoordelijk voor informatiebeveiliging; ICT-beheerders hebben beveiliging in hun takenpakket; lijnmanagers zijn verantwoordelijk voor de beveiliging van de informatie waar zij eigenaar van zijn, en; eindgebruikers moeten zorgvuldig omgaan met hun wachtwoorden. Doordat reeds zoveel rollen bezig zijn met informatiebeveiliging, kan de vraag ontstaan wat de meerwaarde is van een aparte functionaris voor informatiebeveiliging.

Een organisatie binnen de Rijksoverheid heeft op het gebied van informatiebeveiliging taken en verantwoordelijkheden die dienstbaar zijn aan een goede bedrijfsvoering. Enerzijds komt dit vanuit wet- en regelgeving en anderzijds is informatiebeveiliging een intrinsieke verantwoordelijkheid. Uitgaande van de BIR, dient een organisatie die zich wil houden aan algemeen geaccepteerde ‘good practices’, een functionaris verantwoordelijk te maken voor informatiebeveiliging.

Het voordeel van het belegen van taken en verantwoordelijkheden betreffende informatiebeveiliging bij een CISO is dat deze persoon is vrijgemaakt (of gedeeltelijk is vrijgemaakt bij parttime invulling) voor deze taak en een organisatiebrede kijk op beveiliging heeft. Door de snelle veranderingen op het gebied van ICT, de afhankelijkheid van organisaties van digitale informatie, digitale ondersteuning van processen en de potentiële risico’s van overheidsorganisaties bij een tekortkomende informatiebeveiliging, is het belangrijk een medewerker te hebben die volledig is vrijgemaakt om informatiebeveiliging aandacht te geven.

De CISO zorgt dat er maatregelen getroffen worden waardoor inbreuken op de beveiliging kunnen worden voorkomen. Of, als ze toch voorkomen, de gevolgen geminimaliseerd worden. Op basis van risicoanalyses maakt de CISO de mogelijke schade zichtbaar die een dreiging (bijvoorbeeld een aanval van hackers) kan toebrengen aan bepaalde informatie en de kans dat het gebeurt. Het management moet aangeven welke risico’s zij aanvaardbaar acht en welke risico’s (door maatregelen) moeten worden afgedekt. De CISO heeft kennis van risicoanalyse methoden en kan het management ondersteunen bij het opsporen en, tot aanvaardbare risico’s, terugbrengen van kwetsbaarheden binnen de operatie.

Nieuwe ontwikkelingen binnen de overheid vragen een deskundige bijdrage van een CISO. De CISO helpt organisaties de kaders vast te stellen en uit te dragen waarmee de integriteit, beschikbaarheid en vertrouwelijkheid van de informatie(voorziening) kan worden gewaarborgd.

4 Functieprofiel CISO

4.1 Inleiding

In deze handreiking wordt gesproken over de algemene functienaam Chief Information Security Officer (CISO).[2] Deze benaming ligt het dichtst bij het doel van de functie, namelijk het zorg dragen voor informatiebeveiliging. De vele namen die in de praktijk aan de functie van CISO worden gegeven, vertroebelen dit beeld: Het lijkt om vele functies te gaan, maar feitelijk is het één functie (CISO), met hooguit verschillende accenten (die blijken uit de specifieke functienaam).

Het basisfunctieprofiel zoals dat in dit document wordt beschreven is zowel centraal (bij de centrale staf van een organisatie) als decentraal (bij een bedrijfsonderdeel of dienst) niveau toepasbaar. De centrale functie zal de functionele aansturing van de decentrale functie verzorgen.

Binnen het functieprofiel komen de volgende onderdelen aan de orde:

- functienaam (paragraaf 4.2)
- doel van de functie (paragraaf 4.3)
- plaats in de organisatie (paragraaf 4.4)
- resultaatgebieden (paragraaf 4.5)
- gerelateerde functies aan informatiebeveiliging (paragraaf 4.6)
- opleiding, kennis, ervaring en competenties (paragraaf 4.7)
- functiewaardering (paragraaf 4.8)

4.2 Functienaam

De keuze voor een bepaalde functienaam voor een CISO hangt samen met de cultuur van een organisatie en de meer concrete invulling van de functie die de organisatie voor ogen heeft.

Bij dat laatste is er sprake van twee hoofdrichtingen: (1) een organisatorisch gerichte en (2) een technisch gerichte functie. De organisatorisch gerichte gaat over het beleid, de coördinatie en de samenhang van beveiliging. De technisch gerichte houdt zich bezig met (de uitvoering van) één of meer technische beveiligingsonderwerpen. Deze tweedeling sluit overigens ook aan bij de opleidingen die op het gebied van informatiebeveiliging worden gegeven.

[2] Andere mogelijke functienamen voor een CISO zijn onder meer: Informatiebeveiligingsfunctionaris (IBF), beveiligingsadviseur, adviseur informatiebeveiliging, beleidsmedewerker (informatiebeveiliging), Coördinator Informatiebeveiliging, Security Manager, Security Officer, Information Security Manager, Corporate Information Security Officer (CISO), Central Information Security Officer, risico-analist, continuïteitscoördinator, autorisatiebeheerder.

Verder zal bij grotere organisaties, met meer dan één CISO, in de functienaam vaak de plaats binnen de organisatie terugkomen (bijvoorbeeld Local Information Security Officer en Central Information Security Officer). Bij kleinere organisaties (tot ong. 600 medewerkers), waar het bijvoorbeeld gaat om een parttime functie, kan een combinatie plaatsvinden met een verwante (staf)functie. Dat kan dan leiden tot een meer algemene functiebenaming (bijvoorbeeld beleidsmedewerker).

4.3 Doel van de functie

Het doel van de functie is het, op basis van de algemeen aanvaarde BIR, zorg dragen voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen een organisatie. Risicoanalyse, oog voor de bedrijfsvoering en in achtneming van de wettelijke voorschriften zijn daarbij sleutelbegrippen.

Een organisatie heeft meestal beide typen CISO's, de organisatorisch gerichte en de technisch gericht, nodig.

Het doel van de meer technisch gerichte functie is, om met de bij de functie behorende specialistische kennis en kunde het beveiligingsrisico (dus het risico dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van informatie wordt aangetast) als gevolg van de toepassing van (nieuwe) technologieën op een aanvaardbaar niveau te brengen en te houden. Deze functie heeft een rol bij enerzijds de ontwikkeling van nieuwe projecten/systemen, en anderzijds het onderhoud en beheer van bestaande systemen, applicaties en infrastructuur.

De meer beleidsmatig gerichte functie heeft als belangrijkste doel om binnen de organisatie voldoende organisatorische beveiligingsmaatregelen te initiëren, en wel zodanig dat de technische beveiligingsmaatregelen ook daadwerkelijk effectief zijn. Er dient zorg gedragen te worden voor samenhang tussen de technische en organisatorische maatregelen.

Het is mogelijk dat de CISO zich zowel met beleid als uitvoering bezighoudt. Dit is niet wenselijk doordat dit er toe kan leiden dat één van beide gebieden te weinig aandacht krijgt.

4.4 Plaats in de organisatie

Door de breedte aan taken en verantwoordelijkheden van een CISO, kan de functie op verschillende plaatsen in een organisatie worden opgehangen. De plaats in de organisatie hangt samen met de inrichting van de functie en de grootte van de organisatie. De positie van CISO dient een zekere, voor de functie noodzakelijke, onafhankelijkheid ten opzichte van functies in de organisatorische lijn te waarborgen. Korte lijnen naar het management zijn van belang om voldoende bestuurlijk gewicht in de schaal te kunnen leggen, dat nodig voor het treffen en handhaven van voldoende beveiligingsmaatregelen.

De functie van CISO betreft een adviserende staffunctie die direct past onder de directie. De CISO-rol positioneren bij de (ICT-)auditfunctie heeft niet de voorkeur, omdat controle/toezicht door de (ICT-)auditor op de CISO daardoor wordt bemoeilijkt. In dergelijke gevallen dient de externe auditfunctie (bv. door de accountant) een grotere rol te krijgen. Een positionering als staffunctionaris bij een ICT-directeur, informatiemanager of Chief Information Officer (CIO) is

mogelijk. Essentieel is in alle gevallen dat er altijd de mogelijkheid bestaat tot directe rapportage aan de directie van de organisatie. Een risico van plaatsing bij een ICT-directie is dat de nadruk meer op de technische aspecten van informatiebeveiliging komt te liggen, terwijl juist de mensen in een organisatie veelal de zwakke schakel blijken te zijn.

Afhankelijk van de grootte van een organisatie is het mogelijk om naast een CISO op centraal niveau ook decentraal CISO's aan te stellen. Zij ressorteren direct onder het decentrale management. Functioneel worden zij aangestuurd door de CISO op centraal niveau. Bij een kleine organisatie zal er meestal sprake zijn van één CISO, soms zelfs parttime. Als een parttime rol van CISO wordt gecombineerd met andere taken, dan is het belangrijk dat de rollen qua taken, bevoegdheden en verantwoordelijkheden bij elkaar passen. Ook moet de positionering van die andere functie conform de gewenste positionering van de CISO-functie zijn. Een combinatie met aan informatiebeveiliging gelinieerde rollen in een organisatie als risico-, veiligheids-, continuïteits-, privacy en/of kwaliteitsmanagement kan de functie op een hoger plan brengen. Ook een combinatie met een rol als enterprise architect of een rol in de crisisorganisatie is denkbaar.

Een CISO met leidinggevende verantwoordelijkheden binnen zijn beveiligingsrol komt meestal alleen voor in heel grote organisaties, waarbij de functie van CISO door verschillende personen wordt uitgeoefend. In veel gevallen is een CISO alleen een functioneel leidinggevende van decentrale CISO's.

4.5 Resultaatgebieden

De taken en werkzaamheden van een CISO betreffen een aantal resultaatgebieden die beschreven staan in de BIR. Hieronder worden de belangrijkste taken en werkzaamheden op de beschreven gebieden beleid en coördinatie, controle en registratie, communicatie en voorlichting, en advies en rapportage beschreven. Per resultaatgebied worden enkele aandachtspunten bij de taken en werkzaamheden beschreven.

Beleid en coördinatie

De taken en verantwoordelijkheden op het gebied van beleid en coördinatie betreffen:

- Het opstellen en actualiseren van het informatiebeveiligingsbeleid (langere termijn).
- Het (laten) opstellen van informatiebeveiligingsplannen voor afdelingen of deelgebieden (jaarplannen). Het coördineren van de werkzaamheden van personen, afdelingen en instanties die betrokken zijn bij de uitvoering van het informatiebeveiligingsbeleid.
- Het organiseren van en deelnemen aan een coördinerend overleg met betrekking tot informatiebeveiliging.
- Het volgen van nieuwe ontwikkelingen en wetgeving op het gebied van informatiebeveiliging.
- De organisatie vertegenwoordigen in externe gremia.

Aandachtspunten:

Een functiescheiding tussen uitvoering, en controle op de uitvoering is wenselijk.

Door de mogelijke overlap tussen functiegebieden informatiebeveiliging, fysieke beveiliging en privacy dient er algemene coördinatie over deze onderwerpen te worden vormgegeven.

Controle en registratie

De taken en verantwoordelijkheden op het gebied van controle en registratie betreffen:

- Het toezicht houden op de implementatie en naleving van het informatiebeveiligingsbeleid.
- Het opstellen van een controleplan, evenals het leveren van ondersteuning bij het uitvoeren van de daarin gedefinieerde taken.
- Het uitvoeren of initiëren van risicoanalyses en interne audits.
- Het verzamelen en registreren van informatie over de aanwezige beveiligingsmaatregelen.
- Het opzetten of initiëren van een registratie voor beveiligingsincidenten, evenals het afhandelen van opgetreden incidenten en het nemen van preventieve maatregelen ter voorkoming van dergelijke incidenten.

Aandachtspunten:

Informatiebeveiliging is een aspect dat door een hele organisatie heen loopt. Beveiliging betreft de infrastructuur, de applicaties, de processen, de beheerders, management en de gebruikers. Door de breedte van het onderwerp kan het uitzetten en uitvoeren van informatiebeveiliging binnen een organisatie verschillende belangen opleveren.

Communicatie en voorlichting

De taken en verantwoordelijkheden op het gebied van communicatie en voorlichting betreffen:

- Het verzorgen en coördineren van voorlichting en interne opleidingen van het personeel op het gebied van informatiebeveiliging.
- Het stimuleren van het beveiligingsbewustzijn en het opstellen, uitvoeren en onderhouden van een communicatieplan.
- Het onderhouden van externe en interne contacten op alle niveaus binnen dit resultaatgebied.

Advies en rapportage

De taken en verantwoordelijkheden op het gebied van advies en rapportage betreffen:

- Het geven van gevraagd en ongevraagd advies aan bestuur en/of verantwoordelijk (lijn)management van de organisatie ten aanzien van informatiebeveiliging.
- Het rapporteren aan de directie over het gevoerde beleid met betrekking tot informatiebeveiliging, de voortgang van implementatie van nieuwe maatregelen, opgetreden incidenten, ondernomen acties, resultaten van onderzoeken en resultaten van controles.
- Het optreden als projectmanager bij beveiligingsprojecten, waarbij aansturing wordt gegeven aan projectleiders binnen organisatorische eenheden.
- Het afstemmen van informatiebeveiliging met lopende projecten binnen de organisatie.
- Het uitwerken van beveiligingsplannen ten aanzien van de maatregelen, evenals het leveren van ondersteuning bij het uitvoeren van de geaccepteerde plannen.

Aandachtspunten:

De CISO is binnen een organisatie de functionaris bij uitstek op het gebied van informatiebeveiliging. Bij de invoering van nieuwe of vernieuwde systemen, de toepassing van nieuwe technologieën, procedures, maar ook als bepaalde zaken in de praktijk niet goed blijken te lopen, dient de CISO zo vroeg mogelijk te worden ingeschakeld. Informatiebeveiliging in infrastructuur en applicaties achteraf inbouwen is namelijk vaak een lastige en kostbare zaak.

Het is wenselijk dat een CISO zich aansluit bij een kenniskring van vakgenoten, zoals het Platform voor Informatiebeveiliging (PvIB). Op dit moment wordt er nagedacht over een overheid informatiebeveiliging community. Het is voor een CISO belangrijk om op de hoogte te blijven van nieuwe technologische ontwikkelingen.

Rapporteren is een belangrijk onderdeel van de taak van een CISO. Duidelijke en tijdige rapportages zorgen ervoor dat het management weet wat er op het gebied van informatiebeveiliging speelt. Hierdoor blijft het management commitment behouden, dat essentieel is voor het borgen en uitvoeren van informatiebeveiliging in de organisatie.

4.6 Gerelateerde functies aan informatiebeveiliging

Binnen een organisatie zijn er naast de CISO nog een aantal denkbare functies die zich bezighouden met aan informatiebeveiliging gerelateerde gebieden. Een aantal functies kunnen in de praktijk overlappen met de CISO-rol of kunnen zelfs door één medewerker worden uitgevoerd. Voorbeelden van dergelijke functies zijn:

- **De ‘Functionaris voor de Gegevensbescherming’ (FG)/Privacy Officer**

De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens (Wbp). De wettelijke taken en bevoegdheden van de FG

geven deze functionaris een onafhankelijke positie in een organisatie. Een organisatie is niet verplicht een FG te hebben, maar het geeft wel bepaalde voordelen.[3]

De functie van FG kan eventueel worden gecombineerd met de functie van CISO. In ieder geval moet er onderling overleg zijn. Het aspect 'vertrouwelijkheid van informatie' behoort immers ook tot het taakgebied van de CISO.

- **De (ICT-)auditor**

De auditor voert onafhankelijk controleactiviteiten uit, veelal in nauwe samenwerking met de externe accountant. Er is afstemming nodig met betrekking tot de planning van activiteiten. De CISO wordt geïnformeerd over de uitkomsten van de controles. De auditor kan zich bij zijn/haar controles voor een deel baseren op de door de CISO uitgevoerde controles en voortgangsrapportages.

- **De (bedrijfs)beveiliger, portier**

Deze functionaris is belast met de fysieke beveiliging van gebouwen en ruimten binnen een organisatie. Er is zeker een relatie met informatiebeveiliging, bijvoorbeeld daar waar het de beveiliging van computerruimten betreft. In de BIR is fysieke beveiliging ('het voorkomen van ongeautoriseerde toegang tot, schade aan, of verstoring van de gebouwen en informatie van de organisatie) één van de onderwerpen voor informatiebeveiliging. Als gebouwen toegankelijk zijn voor het publiek dient de CISO zich te richten op zoveel mogelijk fysieke en logische beveiliging bij de bron. Door niet de ruimte tot werkplekken beveiligen, maar het apparaat (laptop) zelf.

- **Directeur ICT, informatiemanager, Chief Information Officer**

Deze functie is verantwoordelijkheid ten aanzien van ICT-beleid waar informatiebeveiliging ondersteunend aan is.

- **Personeelsfunctionaris**

Personeelszaken is medeverantwoordelijk voor de selectie en ontslag van personeel, inclusief het personeel dat werkt aan informatiebeveiliging. Ook bij het opstellen van gedragsregels met betrekking tot 'het veilig omgaan met informatie' is er een raakvlak met informatiebeveiliging. Tenslotte kan personeelszaken een belangrijke bijdrage leveren aan informatiebeveiliging door te zorgen dat bij beoordelingsgesprekken met medewerkers expliciet beoordeeld wordt op, de wijze waarop de betreffende medewerker met zijn/haar verantwoordelijkheid ten aanzien van de beveiliging van informatie van de organisatie is omgegaan.

[3] Meer informatie en het openbaar register van FG's is te vinden op de site van het College Bescherming Persoonsgegevens (CBP) (www.cbpweb.nl).

- **Juridische zaken**

Op het gebied van informatiebeveiliging is veel wet- en regelgeving. In het uiterste geval kan het management van een organisatie aansprakelijk worden gesteld als zij onvoldoende heeft gedaan aan informatiebeveiliging. De CISO dient bij het opstellen van beleid en de implementatie van maatregelen bij juridische zaken te toetsen of daarmee wordt voldaan aan alle geldende wet- en regelgeving.

- **Persvoorlichter**

Met het oog op mogelijke beveiligingsincidenten kan het raadzaam zijn dat er overleg is tussen de CISO en de persvoorlichter, en eventueel een jurist, over hoe in voorkomende gevallen extern gecommuniceerd zal gaan worden.

- **Kwaliteitsfunctionaris**

Kwaliteitszorg richt zich op de continue verbetering van de bedrijfsprocessen teneinde de gewenste kwaliteit te kunnen leveren. Informatiebeveiliging richt zich op de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Daarmee levert de CISO een bijdrage aan de kwaliteit van de bedrijfsvoering waardoor overleg en afstemming noodzakelijk is.

4.7 Opleiding, kennis, ervaring en competenties

De volgende functie-eisen zouden aan een CISO gesteld kunnen worden:

Opleiding, kennis en ervaring

- Minimaal HBO/Academisch werk- en denkniveau;
- Kennis en ervaring op het gebied van bestuurskunde en/of informatica;
- Kennis van de actuele stand van zaken en mogelijkheden van ICT (besturingssystemen, netwerken, standaarden, ontwikkel- en beheermethoden);
- Kennis en ervaring op het gebied van informatiebeveiliging en risicoanalyse methoden;
- Kennis van de Baseline Informatiebeveiliging Rijksdienst (BIR) en de ISO 27001/27002;
- Kennis van specialistische beveiligingstechnieken, zoals encryptie;
- Kennis en ervaring op het gebied van adviseren en organisatiekunde;
- Kennis en ervaring op het gebied van de organisatie;
- Kennis van technische infrastructuur samen met de business inschatting van de kwetsbaarheid;
- Kennis en ervaring met projectmatig werken en projectmanagement.

Competenties

Met competenties wordt bedoeld het in staat zijn om weloverwogen de juiste kennis, vaardigheden en houding in te zetten op het juiste moment in authentieke situaties. De volgende functie gerelateerde competenties zouden aan een CISO verwacht mogen worden:

- Goede communicatieve vaardigheden, zowel mondeling als schriftelijk;
- Goed kunnen samenwerken met verschillende disciplines op verschillende niveaus;
- Alert, initiatiefrijk, omgevingsbewust;
- Integer;
- Overtuigend;

4.8 Functiewaardering

In veel organisaties is er geen bestaande functiewaardering voor een CISO, of een vergelijkbare functie. De inschaling blijkt in de praktijk veelal afhankelijk te zijn van de functie waaraan de taak van CISO is toebedeeld. Daarbij kan het bijvoorbeeld gaan om de volgende functies: beleidsmedewerker, stafmedewerker, informatiemanager.

De functie waaraan de taak van CISO wordt toebedeeld, is in die zin van belang dat de plaats van die functie in het organisatie ook de plaats van de CISO-functie binnen de organisatie bepaalt. En zoals elders vermeld, is de positie binnen de organisatie deels bepalend voor het welslagen van de functie.

Onderstaand is een op de huidige praktijk gebaseerde indicatie voor inschaling:

	Meer technisch	Meer organisatorisch
Kleinere organisatie (tot ong. 600 medewerkers	10/11	11/12
Grote organisatie	11/12	12/13

Bijlage: Basisprofiel functie CISO

Functienaam

Algemene functienaam: CISO.

Doel van de functie

Het op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR) zorg dragen voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen een organisatie.

Plaats in de organisatie

Het betreft een staffunctie.

Organigram van de organisatie (inclusief de beveiligingsorganisatie) opnemen.

Resultaatgebieden (taken, werkzaamheden)

- Beleid en coördinatie
- Controle en registratie
- Communicatie en voorlichting
- Advies en rapportage

Aangeven op welke informatiebeveiligingsgebieden uit de Baseline Informatiebeveiliging Rijksdienst deze werkzaamheden concreet betrekking hebben.

Verantwoordelijkheden en bevoegdheden

De belangrijkste bevoegdheid is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen naar de informatiebeveiliging en zo nodig maatregelen voor te schrijven.

Contacten

Zowel interne als externe contacten kunnen onderhouden.

Opleiding, kennis en ervaring

- Minimaal HBO/Academisch werk- en denkniveau;
- Kennis en ervaring op het gebied van bestuurs-/bedrijfskunde en/of informatica;
- Kennis van de actuele stand van zaken en mogelijkheden van ICT (besturingssystemen, netwerken, standaarden, ontwikkel- en beheermethoden);
- Kennis en ervaring op het gebied van informatiebeveiliging en risicoanalyse methoden;
- Kennis van de Baseline Informatiebeveiliging Rijksdienst (BIR) en de ISO 27001/27002;

- Kennis van specialistische beveiligingstechnieken, zoals encryptie;
- Kennis en ervaring op het gebied van adviseren en organisatiekunde;
- Kennis en ervaring op het gebied van de organisatie;
- Kennis van technische infrastructuur samen met de business inschatting van de kwetsbaarheid;
- Kennis en ervaring met projectmatig werken en projectmanagement.

Competenties

- Goede communicatieve vaardigheden, zowel mondeling als schriftelijk;
- Goed kunnen samenwerken met verschillende disciplines op verschillende niveaus;
- Alert, initiatiefrijk, omgevingsbewust;
- Integer;
- Overtuigend;
- Bereid tot permanente scholing.

Functiewaardering

Afhankelijk van de zwaarte: schaal 10, 11, 12 of 13