Bijlage 6

INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie

Handreiking

Handreiking functieprofiel Chief Information Security Officer (CISO)

Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document

Handreiking functieprofiel Chief Information Security Officer (CISO)

Versienummer

2.0

Versiedatum

Juli 2019

Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Rechten en vrijwaring

Met dank aan

De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie

Versie	Datum	Wijziging / Actie
1.0	Augustus 2016	Publicatieversie eerste functieprofiel
2.0	Juli 2019	Actualisatie n.a.v. verplichting volgend uit de BIO

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Leeswijzer

Dit product is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

Doel

Het doel van dit document is gemeenten een handreiking te bieden voor het vormgeven van de CISO-functie binnen hun organisatie of gemeentelijk samenwerkingsverband. De taken, verantwoordelijkheden en bevoegdheden van de functie worden beschreven in relatie tot het lijnmanagement en bestuur binnen de organisatie. Daarnaast wordt de rol van de CISO in relatie tot andere beveiligingsfuncties beschreven, zodat een beeld ontstaat van de samenhang van de CISO-rol met andere rollen binnen de beveiligingsorganisatie.

Doelgroep

Dit document is van belang voor de CISO, het management van de gemeente en de afdelingen HRM en Communicatie.

Relatie met overige producten

- Baseline Informatiebeveiliging Overheid (BIO): hoofdstuk 6 Organiseren van informatiebeveiliging
- Informatiebeveiligingsbeleid van de gemeente
- Handreiking Risicomanagement door lijnmanagers
- Factsheet Informatiebeveiliging voor lijnmanagers

Inhoudsopgave

1. Inleiding

In augustus 2016 is een handreiking IB-functieprofiel voor de Chief Information Security Officer (CISO) gepubliceerd door de Informatiebeveiligingsdienst (IBD), met het doel ondersteuning te geven bij het inrichten van de IB-functie binnen een gemeente. Voor het succesvol implementeren van informatiebeveiliging in een organisatie is de verdeling van verantwoordelijkheden en bevoegdheden voor het beslissen, adviseren en controleren van en over informatiebeveiligingsmaatregelen een basisvoorwaarde. Ontwikkelingen als de invoering van de overheidsbrede Baseline Informatiebeveiliging Overheid (BIO) en de introductie van een eenduidig verantwoordingsstelsel voor informatiebeveiliging (ENSIA) bij gemeenten zijn van invloed op de CISO-functie en rechtvaardigen een actualisatie van het functieprofiel. Daarnaast heeft de functie van CISO zich in het vakgebied informatiebeveiliging steeds meer ontwikkeld als beroep. Die ontwikkeling opent mogelijkheden tot professionalisering en kwalificatie, die we in deze handreiking verkennen.

1.1 Aanstelling CISO is verplichte overheidsmaatregel

Gemeenten verschillen van elkaar qua organisatie en daardoor in de wijze waarop de CISO functie wordt ingevuld. Met de invoering van de BIO en het verbindend verklaren van dit normenkader voor de hele overheid, is aanstelling van een CISO niet langer vrijblijvend, maar verplicht geworden. De aanstelling van een CISO is een belangrijke voorwaarde om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.
Hoe de functie wordt ingevuld beschrijft de BIO niet. In de praktijk is de rol van CISO soms ingevuld als onderdeel van een andere functie. Het komt ook voor dat de CISO een oriëntatie heeft op de meer technische aspecten van informatiebeveiliging (IB), of juist meer gericht is op de organisatie van IB. Toch is er op basis van de taken die in een beveiligingsorganisatie aan de CISO-functie zijn verbonden een basisprofiel op te stellen. Dit basisprofiel voldoet aan het geheel van taken dat op concernniveau aan de CISO-functie verbonden is. Het kan per gemeentelijke organisatie verschillen of deze taken integraal door de CISO worden uitgevoerd, dan wel gedeeltelijk zijn toegewezen aan andere IB-functies, dan wel als rol binnen een andere functie worden uitgevoerd.

1.2 Werkwijze en leeswijzer

In het volgende hoofdstuk wordt het speelveld van de CISO binnen de gemeentelijke organisatie verkend. In het daaropvolgende hoofdstuk wordt een beschrijving gegeven van een functieprofiel voor de CISO. Dit profiel is ontleend aan een rapport[1] van het Platform voor Informatiebeveiliging (PvIB), waarin een uitwerking heeft plaatsgevonden van een Europees raamwerk voor het bepalen van benodigde competenties in het IT-domein. Deze uitwerking is bedoeld om een uniforme basis te bieden voor kwalificatie van de verschillende functies.
In het vervolg van deze handreiking wordt ingegaan op de taken en werkzaamheden van de CISO aan de hand van het door PvIB opgestelde beroepsprofiel. Daarna wordt ingegaan op de mogelijkheden tot certificering van de functie en opleidingen. Tenslotte wordt een drietal normfuncties gepresenteerd, die gebruikt kunnen worden om tot een waardering van de functie binnen de eigen organisatie te komen.

1 1 QIS/PvIB 'Beroepsprofielen informatiebeveiliging 2.0. Een basis voor uniforme kwalificatie van informatiebeveiligers'

2. Het gemeentelijke speelveld van de CISO

2.1 Positionering binnen de organisatie

Een goede positionering van de CISO-functie betekent in elk geval dat de CISO een onafhankelijke positie heeft tegenover zowel het lijnmanagement als het bestuur van de gemeente. De CISO moet midden in de organisatie staan, een directe rapportagelijn hebben naar de (eindverantwoordelijke) gemeentesecretaris en de (bestuurlijk) portefeuillehouder en daarmee periodiek overleg hebben. Daarnaast dient de CISO verbonden te zijn met de ambtelijke organisatie en inzicht te hebben in het primaire proces. De CISO heeft als uitdaging om soms tegengestelde bedrijfs- en beveiligingsbelangen met elkaar te verenigen. Dat vereist een generalistische kijk op informatiebeveiliging en een flexibele benadering van verschillende stakeholders binnen de organisatie.

2.2 Afbakening van de functie

In deze handreiking wordt uitgegaan van een basisfunctieprofiel voor een CISO. Dit profiel is zowel op centraal (concern)niveau toepasbaar als op decentraal niveau. Bij invulling op decentraal niveau is een nader onderscheid te maken tussen een organisatorisch gerichte en een technisch gerichte functie. Dit onderscheid doet zich met name voor in grotere organisaties, waarbij de informatiebeveiligingsfunctie wordt ingericht op domeinniveau. In de praktijk wordt in dat geval vaak gesproken van een Information Security Officer (ISO). De organisatorische functie is daarbij met name gericht op het vertalen van het concernbrede informatiebeveiligingsbeleid naar de specifieke dreigingen, risico's en maatregelen binnen het betreffende domein. Dat is de beleidskant. De technisch gerichte functie is met name gericht op de uitvoering van technische beveiligingsmaatregelen. Dat is de uitvoeringskant.

De concern-CISO fungeert als een programmamanager informatiebeveiliging die overzicht houdt over de concernbrede informatiebeveiliging. Het betreft een staffunctie direct onder het College van B&W of de gemeentesecretaris. De concern-CISO adviseert over en ontwikkelt beleid op meerdere complexe en brede vakgebieden op concern managementniveau. Hij zorgt voor organisatiebrede afstemming en samenhang ten aanzien van vraagstukken en processen die strategisch dan wel tactisch van aard zijn. De domein-ISO heeft specifieke inhoudelijke kennis van de uitvoeringsprocessen binnen het betreffende domein en ondersteunt de proceseigenaar bij het uitvoeren van de risicoafweging en het bepalen van beveiligingsmaatregelen.

2.3 Samenhang met andere functies

Gemeenten zijn de afgelopen jaren geconfronteerd met het ontstaan van nieuwe of versterking van bestaande functies, voortkomend uit nieuwe of gewijzigde wet- en regelgeving, zoals de CISO, de ENSIA-coördinator en de Functionaris Gegevensbescherming. Zeker in kleine gemeenten is daaruit de vraag ontstaan of deze functies als rollen of taakvelden konden worden samengevoegd of worden uitbesteed naar een regionaal samenwerkingsverband. Samenvoeging of uitbesteding van functies is in principe altijd mogelijk, mits functies elkaar qua taken, verantwoordelijkheden en bevoegdheden niet 'bijten'. Er moet in elk geval rekening worden gehouden met het doel van de verschillende functies, omdat dit de genoemde functies wezenlijk onderscheidend maakt van elkaar. Wat de functies gemeenschappelijk hebben, is de onafhankelijkheid van het management en het bestuur in de uitvoering van werkzaamheden die aan de functies verbonden zijn. Maar qua doel verschillen de functies wezenlijk van elkaar.

ENSIA-coördinator

Waar de CISO een adviserende en ondersteunende taak vervult in het kader van informatiebeveiliging, heeft de ENSIA-coördinator een toezichthoudende en controlerende taak. Vaak is de CISO in een gemeente ook ENSIA-coördinator, omdat de horizontale en verticale verantwoording in het kader van ENSIA goed te combineren is met advisering en rapportage van de CISO aan het college van B&W over de informatiebeveiliging. Maar er zit wel een accentverschil in beide functies. De ENSIA-coördinator is meer een controleur die toezicht houdt op 'compliance', d.w.z. overeenstemming van de beveiligingsorganisatie met een voorgeschreven norm (ENSIA). De CISO geeft alleen advies over mogelijke beveiligingsmaatregelen, maar houdt daarbij nadrukkelijk voor ogen dat het de lijnmanager is die uiteindelijk beslist of een risico waarop een maatregel betrekking heeft wel of niet wordt geaccepteerd. Het combineren van beide functies vraagt dus wel enige lenigheid van de betreffende functionaris om richting het lijnmanagement het onderscheid te behouden tussen 'wat moet' (als ENSIA-coördinator) en 'wat kan' (als CISO).

Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming heeft een wettelijke basis in de Algemene Verordening Gegevensbescherming (AVG). Anders dan CISO en ENSIA-coördinator, die vooral op de interne organisatie gericht zijn, is de FG ook aanspreekpunt voor burgers, die zich in hun wettelijke rechten geschaad voelen. De FG vertegenwoordigt de Autoriteit Persoonsgegevens als toezichthouder op de verwerking van persoonsgegevens binnen de gemeentelijke organisatie. De functie van FG heeft een belangrijke basis in de beveiligingsorganisatie, omdat de betrouwbaarheid van de gegevensverwerking geborgd wordt met organisatorische en technische maatregelen. Maar het combineren van deze functie met de functie van CISO en/of ENSIA-coördinator is niet verstandig. Kennis van informatiebeveiliging is voor een FG minder van belang. Het accent binnen de functie ligt op juiste toepassing en interpretatie van wetgeving. Dat vraagt om juridische kennis, niet om technische kennis. Het combineren van rollen van FG en CISO om tot een volwaardige functie-eenheid te komen is af te raden. Het verdient dan de voorkeur om de FG-functie zuiver te houden door op te schalen naar een regionale invulling.

Privacybeheerder BRP / Beveiligingsfunctionaris Suwinet

Naast eerder genoemde functies zijn ook andere functionarissen binnen een gemeente verantwoordelijk voor een specifiek deel van de informatiebeveiliging. Vanuit wet- en regelgeving wordt op verschillende onderdelen binnen de gemeentelijke organisatie de aanstelling verplicht van functionarissen, die een privacy- of beveiligingsfunctie uitoefenen. De bekendste voorbeelden zijn de privacybeheerder BRP en de beveiligingsfunctionaris Suwinet. Dat roept de vraag op of de privacybeheerder BRP niet tevens de rol van FG kan vervullen en de beveiligingsfunctionaris Suwinet niet tevens CISO kan zijn. Vanuit de oriëntatie die deze functies hebben op privacy c.q. informatiebeveiliging is het antwoord op deze vraag dat er zeker een groeipad mogelijk is, maar uit oogpunt van onafhankelijkheid is er wel aanleiding om kritisch naar het combineren van deze functies te kijken. Zowel de privacybeheerder BRP als de beveiligingsfunctionaris Suwinet vervullen hun functie ondergeschikt aan het lijnmanagement. Dat laat zich slecht combineren met een onafhankelijke advies- of toezichthoudende functie. Deze rollen kunnen wel onderdeel zijn van de werkzaamheden van een domein-ISO.

2.4 Interne stakeholders

De onafhankelijke positie van de CISO in de gemeentelijke organisatie betekent allerminst een geïsoleerde positie. De CISO fungeert als aanspreekpunt voor informatiebeveiliging, zowel voor bestuurders, management als medewerkers. Dat vereist de vaardigheid om dezelfde boodschap op verschillende niveaus uit te dragen in de taal die het betreffende niveau aanspreekt. Een belangrijke taak van de CISO is het in stand houden van de beveiligingsorganisatie, die zich uitstrekt van de bepalers van het informatiebeveiligingsbeleid (het bestuur) tot de uitvoerende medewerkers. Als leidraad voor de inrichting van informatiebeveiliging wordt de Baseline Informatiebeveiliging Overheid (BIO) gehanteerd. In de BIO worden drie hoofdrollen in relatie tot informatiebeveiliging onderscheiden. Ze zijn weergegeven in onderstaande tabel.

Secretaris/algemeen directeur	Als eindverantwoordelijke voor het beveiligingsbeleid in de organisatie is de secretaris/algemeen directeur verantwoordelijk voor de uitvoering van organisatiebrede vraagstukken ten aanzien van informatiebeveiliging.
Proceseigenaar	Onder de proceseigenaar wordt de lijnmanager verstaan die verantwoordelijk is voor de beveiliging van het betreffende proces / informatiesysteem. De proceseigenaar is ook verantwoordelijk voor het vaststellen van het basisbeveiligingsniveau (BBN) dat van toepassing is op het betreffende proces.
Dienstenleverancier	Bedoeld wordt de dienstenleverancier (bijv. SSO) binnen de overheid of organisaties in de markt waaraan de secretaris/algemeen directeur of proceseigenaar (een deel van) de beveiligingstaak inbesteedt respectievelijk uitbesteedt.

Naast deze hoofdrollen is een aantal andere functionarissen te onderscheiden, die voor de CISO een belangrijke stakeholder zijn bij de inrichting van de beveiligingsorganisatie.

College van B&W

Het college van B&W is uiteindelijk verantwoordelijk voor het goedkeuren van het gemeentelijke informatiebeveiligingsbeleid. In dit beleid wordt vastgelegd welke doelstellingen ten aanzien van informatiebeveiliging gerealiseerd moeten worden. Dat bepaalt de 'risicobereidheid' van de gemeente. Het beleid wordt door de CISO vertaald in een beveiligingsplan, waarvan de verdere uitwerking onder verantwoordelijkheid van het lijnmanagement plaatsvindt.

HRM-functionaris

In het gemeentelijke personeelsbeleid moet aandacht zijn voor het belang van informatiebeveiliging. Dit beleid wordt vertaald naar procedures en gedragsregels waaraan medewerkers zich dienen te conformeren. Een voorbeeld is een procedure voor introductie van nieuwe medewerkers. Aangezien de mens de sterkste óf de zwakste schakel is in de beveiligingsketen, is aandacht voor de 'zachte kant' van informatiebeveiliging heel belangrijk. Deze krijgt vorm in de organisatorische maatregelen die voor aanvang, tijdens en na het dienstverband van medewerkers worden getroffen. De HRM-functionaris kan beschouwd worden als een generieke proceseigenaar, die het personeelsbeleid vertaalt naar de benodigde beveiligingsmaatregelen. HRM levert een belangrijke bijdrage aan informatiebeveiliging door te zorgen dat bij beoordelingsgesprekken met medewerkers expliciet beoordeeld wordt op het naleven van regels in het kader van informatiebeveiliging.

Medewerker communicatie

De medewerker c.q. afdeling Communicatie is een belangrijke partner in het bevorderen van het informatiebeveiligingsbewustzijn van medewerkers. Dit kan plaatsvinden door het organiseren van bewustwordingscampagnes en/of het reserveren van ruimte op het gemeentelijke intranet voor beveiligingsadviezen. Daarnaast speelt communicatie een belangrijke rol bij het voorkomen, maar ook het afhandelen van beveiligingsincidenten.

Gebouwenbeheerder

In het kader van fysieke beveiliging van gebouwen en ruimten binnen de gemeentelijke organisatie, met het doel ongeautoriseerde toegang tot, schade aan, of verstoring van de gebouwen en informatie van de gemeente te voorkomen, speelt de gebouwenbeheerder een belangrijke rol. De meeste gemeentelijke gebouwen zijn voorzien van een vrij toegankelijke ruimte en ruimten die beveiligd moeten worden tegen ongeautoriseerde toegang. In overleg met de gebouwenbeheerder en de proceseigenaren moet gekomen worden tot een adequate beveiliging d.m.v. een zoneringsplan.

Hoofd IT-afdeling

Het hoofd van de IT-afdeling is een belangrijke stakeholder met het oog op technische maatregelen in het kader van informatiebeveiliging. Ook als onderdelen van de IT zijn uitbesteed naar externe dienstenleveranciers, is deze functionaris het aanspreekpunt voor de CISO.

Hoofd Documentaire Informatievoorziening

DIV beheert alle informatie binnen de organisatie (denk ook aan het zaaksysteem), veilige postverdeling en -bezorging, bewaartermijnen en vernietiging, registratie, substitutie, etc. Een belangrijke partij als je bezig bent met informatieveiligheid om overzicht te verkrijgen van de verschillende soorten gegevensverwerking (handmatig en digitaal) binnen de organisatie.

2.5 Verantwoordelijkheden

De eindverantwoordelijkheid voor informatiebeveiliging berust bij het college van burgemeester en wethouders, maar deze wordt praktisch vertaald naar de lijnorganisatie. De eigenaar van de informatie die in een gegevensverwerkend systeem wordt vastgelegd (meestal de lijnmanager), is verantwoordelijk voor de informatiebeveiliging van het specifieke proces waarin de gegevensverwerking plaatsvindt. Uitbesteding van diensten verandert niets aan de verantwoordelijkheid van de lijnmanagers voor de beveiliging van het betreffende proces / informatiesysteem. De lijnmanager is de enige die verantwoord kan beslissen over de mogelijk tegenstrijdige belangen tussen informatiebeveiliging, efficiency in de procesvoering en de gebruiksvriendelijkheid van informatiesystemen. De CISO ondersteunt het lijnmanagement vanuit een brede kijk op informatiebeveiliging met kennis over mogelijke beveiligingsmaatregelen en helpt de lijnmanagers bij het vergroten van het informatiebewustzijn bij medewerkers, maar de verantwoordelijkheid voor beveiligingsmaatregelen die in een specifiek proces worden getroffen is voorbehouden aan de lijnmanager. Uiteindelijk is de gemeentesecretaris/algemeen directeur verantwoordelijk voor het geheel van informatiebeveiligingsmaatregelen binnen de gemeentelijke organisatie. Binnen een gemeentelijk samenwerkingsverband is dat het bestuur of de directie van het samenwerkingsverband. Met de invoering van de Baseline Informatiebeveiliging Overheid (BIO) komt de nadruk meer te liggen op risicomanagement als basis voor de beveiliging van informatie en informatiesystemen binnen de context van de bedrijfsdoelstellingen. De CISO helpt de lijnmanagers bij het leggen van de relatie tussen dreigingen en risico's en de mogelijke beheer- en beveiligingsmaatregelen. Daarbij wordt ruimte bij de lijnmanager gelaten om vanuit zijn integrale verantwoordelijkheid voor informatiesystemen binnen zijn organisatieonderdeel maatregelen wel of niet van toepassing te verklaren of aan te scherpen. Aan die keuze ligt een risicoafweging ten grondslag[2]. Uiteindelijk geeft de lijnmanager aan welke risico’s hij accepteert en welke risico’s door maatregelen moeten worden afgedekt.

2.6 Budget voor informatiebeveiliging

Informatiebeveiliging kost geld. Het budget voor implementeren van maatregelen is gekoppeld aan de verantwoordelijkheid van het lijnmanagement. Maar ook de CISO heeft budget nodig om verantwoordelijkheden vorm te geven en het lijnmanagement te kunnen ondersteunen. Het zorgen voor de naleving van het beleid en het organiseren van organisatiebrede beveiligingsmaatregelen kost namelijk ook geld. Het behoort tot de taak van de CISO om het informatiebewustzijn binnen de gehele organisatie te bevorderen, van management tot inhuur en hiervoor diverse activiteiten uit te (laten) voeren. Om dit geheel van informatiebeveiliging vorm te kunnen geven, moet de CISO over een eigen budget beschikken voor informatiebeveiliging van de organisatie. Het benodigde budget moet gerelateerd worden aan de jaarplanning van door de CISO uit te voeren activiteiten.

[2] Zie de handreiking ‘Baselinetoets BBN BIO’ en de handreiking ‘Diepgaande risicoanalyse’ van de IBD.

3. Functieprofiel CISO

3.1 Inleiding

Aanstelling van een CISO is met de invoering van de BIO een verplichte overheidsmaatregel (BIO 6.1.1.3). Rol en verantwoordelijkheden moeten in een functieprofiel zijn vastgelegd en dit profiel moet door het hoogste management zijn vastgesteld. Deze maatregelen accentueren het belang dat de CISO binnen de gemeentelijke beveiligingsorganisatie vervult. In dit hoofdstuk wordt een voorbeeld gepresenteerd voor een functieprofiel.

Beroep, functie, rol of taak?

Een functie betreft gelijksoortige samengebundelde werkzaamheden met een gemeenschappelijk doel. Een beroep is algemener, het betreft een bepaalde bekwaamheid los van de organisatie. Een rol geeft de invloed van de houder weer, het is de factor in een proces (bijvoorbeeld: aanjager, voorzitter).
Bij taken gaat het om werkzaamheden, oftewel de operationele inhoud van een functie. De term 'rol' wordt niet gebruikt zoals hierboven gedefinieerd. Zo kan men bijvoorbeeld lezen over de beleidsfunctionaris die de rol van CISO heeft. Beter zou zijn de beleidsfuncionaris die taken uitvoert op het gebied van informatiebeveiliging.

CISO is volgens de voorgaande definitie een beroep. Maar het is ook een functie binnen een organisatie. Daarbij betreft het alle werkzaamheden die tot doel hebben de informatiebeveiliging binnen een organisatie op voldoende niveau te brengen en te houden.

3.2 Doel van het functieprofiel

In opdracht van het platform voor informatiebeveiliging (PvIB) en het programma Qualification of Information Security (QIS) is in 2017 een rapport verschenen over beroepsprofielen in de informatiebeveiliging. Binnen het brede vakgebied informatiebeveiliging is onderscheid te maken tussen twee verschillende domeinen, namelijk informatierisico-management en ICT-beveiliging.

- Informatierisicomanagement richt zich op het beveiligen van de informatievoorziening als geheel, door het sturen en beheersen van een organisatie met betrekking tot risico's op het gebied van de informatievoorziening.
- ICT-beveiliging omvat het ontwerpen, implementeren, onderhouden en evalueren van beveiligingsmaatregelen met betrekking tot de ICT (hardware en software).

Voor deze beide domeinen zijn beroepsprofielen[3] beschreven, ten behoeve van uniforme kwalificatie. De werkzaamheden van de CISO vallen in het vakgebied informatierisicomanagement. Voor een beschrijving van de overige beroepsprofielen wordt verwezen naar het rapport van QIS/PvIB. In totaal worden er vier verschillende beroepsprofielen beschreven.

[3] Om aansluiting te behouden bij het PvIB-rapport hanteren we hier de term 'beroepsprofiel', terwijl we het in principe over de invulling van een functie hebben. In het kader van deze handreiking wordt alleen ingegaan op het beroepsprofiel voor de CISO, maar de lezer wordt uitdrukkelijk uitgenodigd om voor de juiste vertaling van dit beroepsprofiel naar de eigen organisatie ook kennis te nemen van de andere beroepsprofielen die in het QIS/PvIB-rapport worden beschreven.

In onderstaande tabel is weergegeven welke beroepsprofielen binnen het vakgebied informatiebeveiliging worden onderscheiden en op welk niveau in de organisatie (strategisch, tactisch, operationeel) deze profielen zijn gepositioneerd.

	Veiligheid van de I-functie (Information risk management)	**Veiligheid van de ICT-functie** (ICT-beveiliging)
Strategisch en/of tactisch	CISO	ICT-beveiligingsmanager
Tactisch en/of operationeel	ISO	ICT-beveiligingsspecialist *

* Het beroep ICT-beveiligingsspecialist kent drie niveaus, genummerd van 1 (mbo-niveau) tot 3 (universitair niveau).

3.3 Gebruik van het functieprofiel

Binnen het domein van informatiebeveiliging zijn veel verschillende functieaanduidingen in omloop. De keuze voor een bepaalde functienaam hangt samen met de cultuur van een gemeente (voorkeur voor Engelse of Nederlandse benamingen, generieke functiebenamingen zoals beleidsmedewerker of specifieke benamingen) en de meer concrete invulling van de functie die voor ogen staat (organisatorisch, technisch of beide). Taken en competenties die typerend zijn voor de uitvoering van de functie op concernniveau zijn uitgewerkt in het standaard beroepsprofiel Chief Information Security Officer. Dit beroepsprofiel moet gezien worden als een kenmerkende beroepsomschrijving, geformuleerd in termen die binnen het vakgebied herkend worden.

Een beroepsprofiel geeft een formele beschrijving van een beroep. Het beschrijft de doelstelling, taken en verantwoordelijkheden van een beoefenaar van het betreffende beroep en specificeert de competenties (kennis en vaardigheden) die de beoefenaar dient te bezitten.

Het beroepsprofiel is *geen* functiebeschrijving, maar een beschrijving die opgenomen *kan* worden in een functiebeschrijving. Het beroepsprofiel is in eerste instantie opgesteld voor middelgrote informatieverwerkende organisaties, waarin informatieverwerking een prominente rol speelt. Deze beschrijving is van toepassing op de meeste gemeenten. Voor kleine gemeenten geldt misschien dat bepaalde taken of competenties, die in het beroepsprofiel vermeld staan, te ‘klein’ zijn om in een functiebeschrijving te worden vastgelegd. Specifieke afwijkingen van het beroepsprofiel zullen voorkomen. Zolang de verschillen niet te groot worden (80/20-regel) blijft het beroepsprofiel van de CISO een goede indicatie geven van de functie en de eisen die daaraan worden gesteld.

3.4 Uitwerking van het beroepsprofiel

In onderstaande tabel is een uitwerking opgenomen van het beroepsprofiel van de CISO, zoals deze is weergegeven in het PvIB-rapport. Waar nodig is van de oorspronkelijke beschrijving afgeweken om een vertaling te maken naar de gemeentelijke context.

Profieltitel	Concern CISO: Chief Information Security Officer
Samenvatting	De Concern CISO definieert het informatiebeveiligingsbeleid en organiseert en stuurt de informatiebeveiliging van de organisatie overeenkomstig de behoeften en de risicobereidheid van de organisatie.
Doelstelling	Definieert het informatiebeveiligingsbeleid, gebaseerd op een risicomanagement-benadering en rekening houdend met het informatiebeveiligingsdreigingsbeeld, trends en organisatiebehoefte. Richt de informatiebeveiligingsorganisatie in, bepaalt de daarvoor benodigde middelen en de inzet hiervan op concrete beveiligingsmaatregelen. Initieert en coördineert de implementatie van informatiebeveiliging voor de gehele organisatie en houdt daar toezicht op. 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 stakeholders beschouwd als de deskundige op het gebied van informatiebeveiliging.
Producten	Is verantwoordelijk voor:
	• Opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen • Het inrichten van de informatiebeveiligingsorganisatie • Het coördineren en adviseren bij afhandelen van beveiligingsincidenten • Afstemming van informatiebeveiliging met andere beveiligingsdomeinen • Het toezien op naleving van de eisen voor informatiebeveiliging • Het bevorderen van het informatiebeveiligingsbewustzijn over de hele organisatie • De voorbereiding op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's o.b.v. het dreigingsbeeld Nederlandse Gemeenten • Het adviseren bij en begeleiden van informatierisicoanalyses • Het uitvoeren van informatiebeveiligingsassessments
	Realiseert:
	• Projectportfolio voor informatiebeveiliging • Organisatiebrede informatiebeveiligingsactiviteiten en -projecten • Monitoring van de relevante risico's voor de organisatie • Monitoring van compliance met beleid en wet- en regelgeving • Gecoördineerde reactie op ernstige informatiebeveiligings- of ICT- incidenten • Organisatiebrede richtlijnen, standaarden, methoden en technieken voor informatie-beveiliging
	Draagt bij aan:
	• Risicomanagementbeleid • Informatiesysteem-governance • Service Level Agreements • Informatiebeveiligingsarchitectuur
Kerntaken	• Definieert het informatiebeveiligingsbeleid voor de organisatie • Organiseert informatiebeveiliging en de daarvoor benodigde expertise • Zorgt voor afstemming tussen informatiebeveiliging met andere beveiligingsdomeinen, waaronder privacybescherming, fysieke beveiliging en continuïteitsmanagement

Profieltitel	Concern CISO: Chief Information Security Officer
	• Zet een informatiebeveiligingscalamiteitenorganisatie op • Coördineert de reactie op ernstige informatiebeveiligings- of ICT-incidenten • Zorgt voor een projectportfolio voor informatiebeveiliging • Initieert en coördineert organisatiebrede informatiebeveiligingsactiviteiten en -projecten • Zorgt voor organisatiebrede richtlijnen, standaarden, methoden en technieken voor informatiebeveiliging • Monitort en borgt de kwaliteit van informatierisicoanalyses, beveiligingsontwerpen en oplossingen • Monitort en borgt het naleven van de eisen en architectuur voor informatiebeveiliging en het consequent toepassen van Security-by-Design en Privacy-by-Design • Monitort en borgt informatiebeveiligingsbewustzijn binnen de organisatie • Monitort de relevante risico's voor de organisatie • Borgt dat de organisatie voldoende voorbereid is op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's • Monitort en borgt de kwaliteit van informatiebeveiligingsassessments • Monitort op basis van assessments, test, reviews en audits in hoeverre de organisatie compliant is met het informatiebeveiligingsbeleid en wet- en regelgeving • Informeert bestuur en management over de status van informatiebeveiliging en incidenten en presenteert verbetervoorstellen
e-Competenties (uit e-CF)	De onderstaande competenties worden toegelicht in bijlage 1.
	D.1. Beleidsontwikkeling informatiebeveiliging
	E.3. Relatiemanagement
	E.8. Informatiebeveiligingsmanagement
Opleiding en ervaring	• Een afgeronde relevante WO-opleiding of daarmee vergelijkbaar niveau van kennis en vaardigheden • Vijf jaar werkervaring in een informatiebeveiligingsberoep • Vijf jaar werkervaring in een politiek bestuurlijke omgeving
KPI	Inzicht in het vereiste niveau van informatiebeveiliging en informatiebeveiligingsbewustzijn gebaseerd op de behoeften en risicobereidheid van de organisatie

3.5 Waardering van de functie

Een groot deel van de gemeenten maakt gebruik van het HR21-systeem om functies in te delen in een gemeentelijk functiehuis. HR21 is een functiewaarderingssysteem dat specifiek voor de gemeentelijke sector is ontwikkeld. Bij de functiewaardering wordt gebruik gemaakt van indelingsmotiveringen, waarbij de indeling plaatsvindt aan de hand van functiekenmerken in een bepaalde normfunctie. Overigens leidt dat niet tot een concrete indicatie van het schaalniveau dat aan de functie verbonden wordt. Gemeenten bepalen zelf welke salarisschaal aan een bepaalde functie wordt verbonden.

Op verzoek van de IBD heeft de HR21-organisatie indelingsmotiveringen opgesteld voor de CISO-functie. Daarbij is onderscheid gemaakt tussen het basisfunctieprofiel, dat in deze handreiking is beschreven, een organisatorische functie binnen een dienst of sector en een meer technisch gerichte functie. De indelingsmotiveringen zijn als bijlage 1 toegevoegd aan deze handreiking.

4. Kwalificatiemogelijkheden

4.1 Inleiding

Het beroepsprofiel van de CISO is opgesteld met het doel hiermee een basis te leggen voor uniforme kwalificatie. Het verwerven van de voor een CISO benodigde competenties kan door het volgen van onderwijs en door het leren in de praktijk.
Het volgen van onderwijs en het leren in de praktijk hebben beide voor- en nadelen. Zo brengt het volgen van onderwijs de beoogde competenties sneller binnen bereik, maar het leereffect blijft veelal beperkt tot de beoogde competenties. Met leren in de praktijk kost het veelal meer tijd om de beoogde competenties te verwerven, maar daarnaast worden ook andere competenties verworven die wellicht niet direct nodig zijn, maar de persoon in kwestie wel een bredere basis geven en daarmee meer flexibiliteit in inzicht en handelen. Vanwege de verschillende voor- en nadelen is het wenselijk om beide mogelijkheden beschikbaar te hebben.

4.2 Kun je leren om 'CISO' te zijn?

Het PvIB-rapport stelt dat aan het 'zware' beroepsprofiel van de concern-CISO hogere eisen worden gesteld dan in een initiële opleiding (HBO, Universitair) verworven kunnen worden. Zo'n startkwalificatie legt wel een stevig fundament, maar daarnaast is het opdoen van werkervaring en het volgen van extra cursussen noodzakelijk. Er zijn genoeg mogelijkheden om in de praktijk de nodige competenties te kunnen verwerven. Maar hoe toets je vervolgens of iemand voldoende competenties heeft om te voldoen aan het beroepsprofiel?
Gemeenten vragen van een CISO verschillende startkwalificaties, variërend van CISA, CISM, CISSP tot Master-opleidingen in het economische, exacte, technische of menswetenschappelijke domein. Die variëteit in de uitvraag geeft aan dat het bij gemeenten nog onvoldoende duidelijk is welke startkwalificatie het beste aansluit bij de functie van CISO. Dat heeft te maken met de relatieve onbekendheid met de inhoud van de functie, maar ook met het feit dat er op dit moment nog geen toetsingsproces is ingericht dat objectief mogelijkheden geeft tot het oordeel dat iemand een 'goede' CISO is. Vooralsnog is het opstellen van een breed gedragen beroepsprofiel voor de CISO nog niet gevolgd door het aanbieden van opleidingen die op dit profiel aansluiten. Maar de basis daarvoor is wel gelegd met het opstellen van het beroepsprofiel.

Op dit moment moet een CISO de professionaliteit hebben om zelf zijn vakmanschap op peil te houden, door kennis en vaardigheden op te doen die nodig zijn voor het anticiperen op de relevante maatschappelijke en technische ontwikkelingen. Welke kennis moet worden opgedaan, hangt af van de 'aanvliegroute' die tot de aanstelling tot CISO heeft geleid c.q. moet gaan leiden. Voor een CISO met een organisatie-achtergrond ligt het voor de hand om kennis te vergaren op ICT-gebied, terwijl de CISO die een meer specialistische ICT-achtergrond heeft juist moet kiezen voor een organisatie en management gerichte oriëntatie. In bijlage 2 is een aantal voorbeelden opgenomen van certificeringen en cursussen die hieraan een bijdrage zouden kunnen leveren.

Zoals in het beroepsprofiel is aangegeven, zijn er naast de kenniscompetenties ook (en misschien wel vooral) algemene competenties van belang voor de CISO. De CISO moet in staat zijn om in een ongestructureerde en onvoorspelbare omgeving zelfstandig tot een (kritisch) advies te komen en in geval van een beveiligingsincident zelfstandig beslissingen kunnen nemen, om daarover later verantwoording af te leggen. Bovendien moet hij verschillende stakeholders 'meekrijgen' in de door hem voorgestelde richting. Binnen de gemeentelijke context is communicatie en overtuigingskracht een voor de CISO noodzakelijke kerncompetentie. Een CISO moet in staat zijn boven soms tegengestelde belangen uit te stijgen en de taal kunnen spreken van zowel de bestuurder als de medewerker. Informatiebeveiliging is '*chefsache*': bestuurders moeten zich eigenaar voelen van informatieveiligheid en dit samen met CISO en gemeentesecretaris vertalen naar concrete maatregelen[4]. Maar de CISO speelt ook een belangrijke rol in het bevorderen van het beveiligingsbewustzijn van medewerkers. Dat vereist een zekere lenigheid van de CISO om het belang van informatiebeveiliging in de juiste bewoordingen onder de aandacht te brengen op verschillende niveaus binnen de organisatie (strategisch, tactisch, operationeel).

4.3 Aansluiten bij de IBD

Voor de CISO binnen het gemeentelijk domein is de aansluiting bij de IBD belangrijk. Aansluiting kan plaatsvinden als VCIB (vertrouwde contactpersoon) [5] of als ACIB (algemeen contactpersoon). De IBD communiceert uitsluitend met de VCIB over vertrouwelijke beveiligingsincidenten. De CISO speelt een belangrijke rol in de afhandeling van deze incidenten.
Het is een must voor elke CISO om zich aan te sluiten bij de IBD Community. Via de IBD Community wordt kennisdeling tussen gemeenten onderling gefaciliteerd. Als CISO binnen het gemeentelijk domein zijn er meer dan 300 collega's waarmee kennis kan worden uitgewisseld. Kennisdeling is in het kader van professionalisering van de functie een belangrijke meerwaarde. Daarnaast is samen optrekken en zo nodig standaardiseren noodzakelijk om aan burgers uit te kunnen leggen dat hun informatie bij 'de overheid' in veilige handen is. De IBD ondersteunt de kennisdeling door leden via de Community:

- Door gemeentelijke beveiligingsdocumenten die door een gemeente beschikbaar zijn gesteld te delen met andere gemeenten;
- Door als mediator op te treden bij vragen en discussies op informatiebeveiligingsvlak;
- Door producten van de IBD in bewerkbare vorm beschikbaar te stellen;
- Door een platform te zijn voor alle IBD-producten.

4 Deze constatering komt uit "Durven leren", Eindrapport van de Visitatiecommissie Informatieveiligheid, september 2017

5 Zie voor een toelichting op beide functies de factsheet "Verantwoordelijkheden van de VCIB"

INFORMATIE
BEVEILIGINGS
DIENST

Bijlage 1 Indelingsmotiveringen HR21

Indelingsmotivering Concern CISO

Voor de functie wordt hieronder aangegeven waarom gekozen is voor de normfunctie in HR21.

Gegevens van de Normfunctie HR21		
Naam	:	Concern CISO: Chief Information Security Officer
Normnaam	:	Adviseur II
Functiereeks	:	Beleid
Functiegroep	:	Advies

Informatie van de huidige functie	
Hoofdtaken	1. Beleid & Coördinatie 2. Controle & Registratie 3. Communicatie & Voorlichting 4. Advies & Rapportage
Context en werkzaamheden	*Concern CISO: organisatiebreed* • Zorgdragen voor het opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen. • Optreden als informatiebeveiligingsadviseur (voor het management) bij nieuwe ICT-voorzieningen en bij ingrijpende veranderingen in de ICTinfrastructuur. • Adviseren van het (lijn)management bij de uitwerking van het informatiebeveiligingsbeleid in informatiebeveiligingsplannen voor hun verantwoordelijkheidsgebieden, en bij de implementatie van deze plannen. • Initiëren of laten uitvoeren van periodieke beveiligingsaudits, risico-, afhankelijkheids- en kwetsbaarheidsanalyses. • Coördineren en adviseren bij beveiligingsincidenten en zo nodig optreden bij calamiteiten. • Op de hoogte blijven van ontwikkelingen op het gebied van informatiebeveiliging en zo nodig met voorstellen komen voor aanvullingen of verbeteringen van producten, methodieken of werkwijzen met betrekking tot de informatiebeveiliging. • Opzetten en initiëren van informatiebeveiligings-bewustzijnprogramma's en adviseren over voorlichting en training van gebruikers in het correct omgaan met informatie(systemen).

VNG Realisatie

	• Te allen tijde een open deur hebben voor de gebruikersorganisatie indien deze, buiten de hiërarchie om, een beveiligingsincident wil melden. De Concern CISO is het formele, en bij iedereen in de organisatie bekende, aanspreekpunt voor 'informatiebeveiligingszaken'. • Projecten leiden met als doel beveiligingsmaatregelen te implementeren of de kwaliteit van de beveiliging op langere termijn te handhaven en verbeteren. • Controleren van de werking en naleving van het informatiebeveiligingsbeleid en daaruit voortvloeiende maatregelen. • Periodiek rapporteren van beveiligingsincidenten en de afhandeling daarvan aan de portefeuillehouder. • De gemeente vertegenwoordigen in externe overleggremia. • Rapportages op het gebied van de beveiliging laten beoordelen.
De omgeving van de functie	De onafhankelijke positie van de CISO in de gemeentelijke organisatie betekent allerminst een geïsoleerde positie. De CISO fungeert als aanspreekpunt voor informatiebeveiliging, zowel voor bestuurders, management als medewerkers. Een belangrijke taak van de CISO is het in stand houden van de beveiligingsorganisatie, die zich uitstrekt van de bepalers van het informatiebeveiligingsbeleid (het bestuur) tot de uitvoerende medewerkers. Als leidraad voor de inrichting van informatiebeveiliging wordt de Baseline Informatiebeveiliging Overheid (BIO) gehanteerd. Belangrijke stakeholders voor de CISO zijn hierbij de secretaris/algemeen directeur van de organisatie als eindverantwoordelijke voor het beveiligingsbeleid, de lijnmanager, de dienstenleverancier (bijv. SSO), het college van B&W, de HRM functionaris, de medewerker communicatie, de gebouwenbeheerder en het Hoofd IT-afdeling. Extern contact is er met auditors/toezichthouders (accountant, ministerie, IBD), service providers en politie/justitie. Extern wisselt de Concern CISO kennis en ervaring uit met vakgenoten van andere gemeenten en met de informatiebeveiligingsdienst (IBD). In dat laatste geval kan de Concern CISO ook VCIB en/of ACIB zijn, of de contacten intern onderhouden met de ACIB/VCIB van de gemeente waar de Concern CISO werkzaam is. Om op de hoogte te blijven van nieuwe technologische ontwikkelingen is contact met leveranciers (beurzen, lidmaatschap gebruikersgroepen van bepaalde producten) tevens van belang.

Motivering keuze in HR21	
Keuze functiereeks	**Beleid**
	Het adviseren over, ontwikkelen, uitvoeren of handhaven van beleidsterreinen en beleidsprocessen.

Motivering van keuze	De Concern CISO is verantwoordelijk voor het opstellen, bijstellen, vernieuwen en herzien van het **informatiebeveiligingsbeleid** en de daaruit voortvloeiende informatie(beveiligings-) plannen. Daarnaast is de Concern CISO verantwoordelijk voor het coördineren van de werkzaamheden van personen, afdelingen en instanties die zijn betrokken bij de uitvoering van het informatiebeveiligingsbeleid.
	De Concern CISO treedt daarnaast op als **informatiebeveiligingsadviseur** (voor het management) bij nieuwe ICT-voorzieningen en bij ingrijpende veranderingen in de ICT-infrastructuur. Tevens adviseert de Concern CISO het management bij de uitwerking van het informatiebeveiligingsbeleid in informatiebeveiligingsplannen voor hun verantwoordelijkheidsgebieden, en bij de implementatie van deze plannen.
Keuze functiegroep	**Advies**
	Advisering en (beleids)ontwikkeling vanuit intern gerichte beleidvelden en processtructuren. Voor de uitvoering geldt een interne opdrachtgeveropdrachtnemer relatie. Resultaten worden getoetst aan interne service level agreements, kwaliteitsnormen, protocollen en/of fundamentele keuzes.
Motivering van keuze	De Concern CISO adviseert over en ontwikkelt het informatiebeveiligingsbeleid vanuit het interne gerichte beleidsveld. De Concern CISO adviseert het management bij de uitwerking van dit informatiebeveiligingsbeleid in plannen voor hun verantwoordelijkheidsgebieden en rapporteert periodiek de beveiligingsincidenten en de afhandeling daarvan aan de portefeuillehouder (interne opdrachtgever).
Keuze functie	**Adviseur II**
	• adviseert over en ontwikkelt beleid op **meerdere complexe en brede** vakgebieden op **concern- en breder managementniveau** • **zorgt voor organisatiebrede afstemming en samenhang** ten aanzien van vraagstukken en processen die **strategisch dan wel tactisch** van aard zijn • zorgt voor de uitvoering en implementatie van **multidisciplinaire** vraagstukken en processen

Motivering o.b.v. overwegende functiekenmerken	De Concern CISO adviseert over en ontwikkelt het informatiebeveiligingsbeleid vanuit het interne gerichte beleidsveld op concern- en managementniveau. Daarnaast zorgt de Concern CISO voor organisatiebrede afstemming (kader stellend op domeinniveau) en samenhang ten aanzien van informatiebeveiligingsvraagstukken en processen die strategisch dan wel tactisch van aard zijn. De CISO draagt zorgt voor samenhang tussen technische en organisatorische maatregelen binnen de gemeente. Dit vereist inzicht in verschillende samenhangende vakgebieden (informatiebeveiliging, ICT, juridisch, privacy etc.). De Concern CISO houdt hierdoor de beveiligingsorganisatie in stand, die zich uitstrekt van de bepalers van het informatiebeveiligingsbeleid (het bestuur) tot de uitvoerende medewerkers.
Motivering o.b.v. resultaatgebieden	• **Resultaatgebied 1: Advies** • **Resultaatgebied 2: Beleidsontwikkeling** • **Resultaatgebied 3: Procesbewaking en regie** • **Resultaatgebied 4: Relatiebeheer**
	Advies • Optreden als projectmanager bij beveiligingsprojecten, waarbij aansturing wordt gegeven aan projectleiders binnen organisatorische eenheden. • Afstemmen van informatiebeveiliging met lopende projecten binnen de organisatie en andere beveiligingsdomeinen. • Uitwerken van beveiligingsplannen ten aanzien van de maatregelen, evenals het leveren van ondersteuning bij het uitvoeren van de geaccepteerde plannen. • Adviseren aan de leiding van de organisatie en het lijnmanagement over de te nemen beveiligingsmaatregelen. • Rapporteren aan de leiding van de organisatie 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. • Informeren van het bestuur en management over de status van informatiebeveiliging/incidenten en het presenteren van verbetervoorstellen.

	2. Beleidsontwikkeling en Coördinatie • Opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen. • Zorgdragen voor de totstandkoming van informatiebeveiligingsplannen voor afdelingen of deelgebieden (jaarplannen). • Coördineren van de werkzaamheden van personen, afdelingen en instanties die zijn betrokken bij de uitvoering van het informatiebeveiligingsbeleid.
	3. Procesbewaking en regie • Toezicht houden op de implementatie en naleving van het informatiebeveiligingsbeleid en eisen voor informatiebeveiliging. • Opstellen van een controleplan, evenals het leveren van ondersteuning bij het uitvoeren van de daarin gedefinieerde taken. • Adviseren bij en begeleiden van informatierisicoanalyses. • Uitvoeren van informatiebeveiligingsassessments of initiëren van risicoanalyses en interne audits. • Monitoren en borgen van de kwaliteit van de informatierisicoanalyses, beveiligingsontwerpen en oplossingen. • Zorgdragen voor de voorbereiding op toekomstige • informatiebeveiligingsrisico's en ICT-beveiligingsrisico's o.b.v. het dreigingsbeeld Nederlandse Gemeenten. • Verzamelen en registreren van informatie over de aanwezige beveiligingsmaatregelen. • 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.
	4. Relatiebeheer • Inrichten van de informatiebeveiligingsorganisatie. • Onderhouden van externe en interne contacten op alle niveaus binnen dit kader. • Verzorgen en coördineren van organisatiebrede voorlichting, activiteiten, projecten en interne opleidingen op het gebied van informatiebeveiliging. • Stimuleren van het informatiebeveiligingsbewustzijn over de hele organisatie. • Volgen van nieuwe ontwikkelingen en wetgeving op het gebied van informatiebeveiliging.

Vergelijking met het hogere en lagere niveau binnen de functiegroep	De naast hogere functie, Adviseur I, adviseert (met een hoog innovatief karakter) over en ontwikkelt beleid op bestuurlijk- en concern niveau en geeft invulling aan vraagstukken op strategisch niveau. Bij de CISO ligt de nadruk meer op strategisch-tactisch niveau. Adviseur I is daarom niet passend. De naast lagere functie, Adviseur III, adviseert op tactisch niveau binnen het eigen vakgebied en is minder bezig met de concern brede samenhang ten aanzien van vraagstukken en processen. Adviseur III is daarom niet passend.

Indelingsmotivering Domein ISO

Voor de functie wordt hieronder aangegeven waarom gekozen is voor de normfunctie in HR21.

Gegevens van de Normfunctie HR21		
Naam	:	Domein ISO: Information Security Officer
Normnaam	:	Adviseur III
Functiereeks	:	Beleid
Functiegroep	:	Advies

Informatie van de huidige functie	
Hoofdtaken	1. Beleid & Coördinatie 2. Controle & Registratie 3. Communicatie & Voorlichting 4. Advies & Rapportage

Context en werkzaamheden	*Domein ISO: domeinbreed* • Bijdragen aan het opstellen bijstellen, vernieuwen en herzien van het organisatiebrede informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen op zijn/haar domein binnen de gemeente. • Optreden als informatiebeveiligingsadviseur (voor het management) bij nieuwe ICT-voorzieningen en bij ingrijpende veranderingen in de ICTinfrastructuur. • Adviseren van het (lijn)management bij de uitwerking van het informatiebeveiligingsbeleid in informatiebeveiligingsplannen voor hun verantwoordelijkheidsgebieden, en bij de implementatie van deze plannen. • Initiëren of laten uitvoeren van periodieke beveiligingsaudits, risico-, afhankelijkheids- en kwetsbaarheidsanalyses. • Coördineren en adviseren bij beveiligingsincidenten en zo nodig optreden bij calamiteiten. • Op de hoogte blijven van ontwikkelingen op het gebied van informatiebeveiliging en zo nodig met voorstellen komen voor aanvullingen of verbeteringen van producten, methodieken of werkwijzen met betrekking tot de informatiebeveiliging. • Opzetten en initiëren van informatiebeveiligings-bewustzijnprogramma's en adviseren over voorlichting en training van gebruikers in het correct omgaan met informatie(systemen). • Te allen tijde een open deur hebben voor de gebruikersorganisatie indien deze, buiten de hiërarchie om, een beveiligingsincident wil melden. De Domein ISO is het formele, en bij iedereen in de organisatie bekende, aanspreekpunt voor 'informatiebeveiligingszaken' binnen zijn/haar domein. • Projecten leiden met als doel beveiligingsmaatregelen te implementeren of de kwaliteit van de beveiliging op langere termijn te handhaven en verbeteren. • Controleren van de werking en naleving van het informatiebeveiligingsbeleid en daaruit voortvloeiende maatregelen. • Periodiek rapporteren van beveiligingsincidenten en de afhandeling daarvan aan de portefeuillehouder. • De gemeente vertegenwoordigen in externe overleggremia. • Rapportages op het gebied van de beveiliging laten beoordelen.

De omgeving van de functie	Intern moet de Domein ISO contact onderhouden met andere ISO's of beveiligingsfunctionarissen binnen een deel van zijn/haar gemeente of een deel van zijn/haar organisatie. De Domein ISO werkt dus niet voor de gehele organisatie breed. De Domein ISO op corporate niveau heeft daarbij de verantwoordelijkheid dit contact te structureren in vaste en ad-hoc overlegvormen. Verder onderhoudt de Domein ISO intern contact met lijnmanagers, projectmanagers en auditors en eventueel Concern CISO. Extern contact is er met auditors/toezichthouders (accountant, ministerie, IBD), service providers en politie/justitie. Extern wisselt de Domein ISO kennis en ervaring uit met vakgenoten van andere gemeenten en met de informatiebeveiligingsdienst (IBD). In dat laatste geval kan de Domein ISO ook VCIB en/of ACIB zijn, of de contacten intern onderhouden met de ACIB/VCIB van de gemeente waar de ISO werkzaam is. Om op de hoogte te blijven van nieuwe technologische ontwikkelingen is contact met leveranciers (beurzen, lidmaatschap gebruikersgroepen van bepaalde producten) tevens van belang.
	De Domein ISO treedt daarnaast op als **informatiebeveiligingsadviseur** (voor het management) bij nieuwe ICT-voorzieningen en bij ingrijpende veranderingen in de ICT-infrastructuur. Tevens adviseert de Domein ISO het (lijn)management bij de uitwerking van het informatiebeveiligingsbeleid in informatiebeveiligingsplannen voor hun verantwoordelijkheidsgebieden, en bij de implementatie van deze plannen.
Keuze functiegroep	**Advies**
	Advisering en (beleids)ontwikkeling vanuit intern gerichte beleidsvelden en processtructuren. Voor de uitvoering geldt een interne opdrachtgeveropdrachtnemer relatie. Resultaten worden getoetst aan interne service level agreements, kwaliteitsnormen, protocollen en/of fundamentele keuzes.

Motivering keuze in HR21	
Keuze functiereeks	**Beleid**
	Het adviseren over, ontwikkelen, uitvoeren of handhaven van beleidsterreinen en beleidsprocessen
Motivering van keuze	De Domein ISO is verantwoordelijk voor het opstellen, bijstellen, vernieuwen en herzien van het **informatiebeveiligingsbeleid** en de daaruit voortvloeiende informatie(beveiligings-) plannen. Daarnaast is de Domein ISO verantwoordelijk voor het coördineren van de werkzaamheden van personen, afdelingen en instanties die zijn betrokken bij de uitvoering van het informatiebeveiligingsbeleid binnen het gedeelde van zijn/haar domein.

Motivering van keuze	De Domein ISO adviseert over en ontwikkelt het informatiebeveiligingsbeleid vanuit het interne gerichte beleidsveld. De Domein ISO adviseert het lijnmanagement en de Concern CISO bij de uitwerking van dit informatiebeveiligingsbeleid in plannen voor hun verantwoordelijkheidsgebieden en rapporteert periodiek de beveiligingsincidenten en de afhandeling daarvan aan de portefeuillehouder (interne opdrachtgever).
Keuze functie	**Adviseur III**
	• adviseert over en ontwikkelt beleid op meerdere **samenhangende** vakgebieden • adviseert over vraagstukken en processen die **tactisch** van aard zijn en die worden gestuurd door beleidsmatige keuzes binnen het vakgebied • zorgt voor de uitvoering en implementatie van **multidisciplinaire** vraagstukken en processen
Motivering o.b.v. overwegende functiekenmerken	De Domein ISO adviseert over en ontwikkelt het informatiebeveiligingsbeleid vanuit het interne gerichte beleidsveld op domeinniveau (binnen de kaders van het op concernniveau bepaalde beleid). Daarnaast adviseert de Domein ISO over informatiebeveiligingsvraagstukken en processen die tactisch van aard zijn. De Domein ISO draagt zorgt voor samenhang tussen technische en organisatorische maatregelen binnen zijn/haar domein binnen de gemeente. Dit vereist inzicht in verschillende samenhangende vakgebieden (informatiebeveiliging, ICT, juridisch, privacy etc.).
Motivering o.b.v. resultaatgebieden	• **Resultaatgebied 1: Advies** • **Resultaatgebied 2: Beleidsontwikkeling** • **Resultaatgebied 3: Procesbewaking en regie** • **Resultaatgebied 4: Relatiebeheer**

1. Advies

- Optreden als projectmanager bij beveiligingsprojecten, waarbij aansturing wordt gegeven aan projectleiders binnen organisatorische eenheden.
- Afstemmen van informatiebeveiliging met lopende projecten binnen het domein van de gemeente.
- Uitwerken van beveiligingsplannen ten aanzien van de maatregelen, evenals het leveren van ondersteuning bij het uitvoeren van de geaccepteerde plannen.
- Geven van gevraagd en ongevraagd advies aan de leiding van de organisatie en het lijnmanagement over de te nemen beveiligingsmaatregelen.
- Rapporteren aan de leiding van de organisatie 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.

2. Beleidsontwikkeling en Coördinatie

- Bijstellen en actualiseren van het informatiebeveiligingsbeleid (langere termijn) op domein niveau a.d.h.v. organisatiebreed informatiebeveiligingsbeleid.
- Opstellen van informatiebeveiligingsplannen voor zijn/haar domein binnen de gemeente (jaarplannen). Het coördineren van de werkzaamheden van personen, afdelingen en instanties die zijn betrokken bij de uitvoering van het informatiebeveiligingsbeleid.

3. Procesbewaking en regie

- Toezicht houden op de implementatie en naleving van het informatiebeveiligingsbeleid en eisen voor informatiebeveiliging.
- Opstellen van een controleplan, evenals het leveren van ondersteuning bij het uitvoeren van de daarin gedefinieerde taken.
- Uitvoeren van informatiebeveiligingsassessments of initiëren van risicoanalyses en interne audits.
- Monitoren en borgen van de kwaliteit van de informatierisicoanalyses, beveiligingsontwerpen en oplossingen, binnen het domein.
- Bijdragen aan de voorbereiding op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's o.b.v. het dreigingsbeeld Nederlandse Gemeenten.
- Verzamelen en registreren van informatie over de aanwezige beveiligingsmaatregelen.
- 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.

	4. Relatiebeheer • Onderhouden van externe en interne contacten op alle niveaus binnen dit kader. • Deelnemen aan een coördinerend overleg met betrekking tot informatiebeveiliging (met Concern CISO of andere ISO's). • Verzorgen en coördineren van voorlichting en interne opleidingen van het personeel binnen het domein op het gebied van informatiebeveiliging. • Stimuleren van het beveiligingsbewustzijn binnen het domein. • Volgen van nieuwe ontwikkelingen en wetgeving op het gebied van informatiebeveiliging.
Vergelijking met het hogere en lagere niveau binnen de functiegroep	De naast hogere functie, Adviseur II, adviseert over en ontwikkelt beleid op bestuurlijk- en concern niveau en geeft geen invulling aan vraagstukken op strategisch dan wel tactisch niveau. Het verschil is dat de Adviseur II dit op concern niveau doet en niet op domein niveau. Adviseur II is daarom niet passend. De naast lagere functie, Adviseur IV, adviseert op tactisch dan wel operationeel niveau binnen het eigen vakgebied en is minder bezig met de samenhang ten aanzien van vraagstukken en processen. Adviseur IV heeft daarnaast meer uitvoerende taken. Adviseur IV is daarom niet passend.

Indelingsmotivering Technische ISO

Voor de functie wordt hieronder aangegeven waarom gekozen is voor de normfunctie in HR21.

Gegevens van de Normfunctie HR21		
Naam	:	Technische ISO: Information Security Officer
Normnaam	:	Systemen II
Functiereeks	:	Beheer
Functiegroep	:	Systemen

Informatie van de huidige functie	
Hoofdtaken	1. Ontwikkeling infrastructuur 2. Systeem-, netwerk- en applicatiebeheer 3. Gebruikersondersteuning
Context en werkzaamheden	• Bijdragen vanuit de praktijk aan het informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen, gericht op de technische kant van de ISO. • Optreden als informatiebeveiligingsadviseur (voor het lijnmanagement) bij nieuwe ICT-voorzieningen en bij lopende, casuïstische vraagstukken in de ICT-infrastructuur. • Bijdragen aan de ontwikkeling van nieuwe projecten/systemen met als doel beveiligingsmaatregelen te implementeren of de kwaliteit van de beveiliging op langere termijn te handhaven en verbeteren. • Onderhoud en beheer van bestaande systemen, applicaties en infrastructuur. • Bijdragen aan informatiebeveiligings-bewustzijnprogramma's en adviseren over voorlichting en training van gebruikers in het correct omgaan met informatiesystemen. • Afhandelen van vragen en klachten van gebruikers binnen de gemeente over de ICT-infrastructuur rondom informatiebeveiliging. • Ondersteunen van gebruikers bij (nieuwe) ICT-voorzieningen en de ICTinfrastructuur rondom informatiebeveiliging, binnen de gemeente. • Periodiek rapporteren van beveiligingsincidenten en de afhandeling daarvan aan de portefeuillehouder en de Concern of Domein ISO. • Rapportages op het gebied van de beveiliging laten beoordelen.

De omgeving van de functie	Intern moet de Technische ISO contact onderhouden met andere Concern en Domein ISO's of beveiligingsfunctionarissen binnen zijn/haar gemeente. Ook rapporteert hij/zij aan de Concern CISO. Verder onderhoudt de Technische ISO intern contact met lijnmanagers, projectmanagers en auditors. Om op de hoogte te blijven van nieuwe technologische ontwikkelingen is extern contact met leveranciers (beurzen, lidmaatschap gebruikersgroepen van bepaalde producten) van belang.

Motivering keuze in HR21	
Keuze functiereeks	**Beheer**
	Uitvoeren van beheersmatige werkzaamheden met betrekking tot locatie(s), systemen, gegevens en bedrijfsvoering.
Motivering van keuze	De Technische ISO draagt vanuit de technische praktijk bij aan het informatiebeveiligingsbeleid en voert beheersmatige werkzaamheden uit met betrekking tot (nieuwe) ICT-voorzieningen en de ICT-infrastructuur rondom informatiebeveiliging, binnen de gemeente. Tevens adviseert de Technische CISO het (lijn)management over de praktische toepassing hiervan.
Keuze functiegroep	**Systemen**
	Het uitvoeren van beheersmatige werkzaamheden met betrekking tot ICT-systemen, netwerken en/of applicaties. Binnen de functiegroep ligt het accent op inrichten en beheren, het hierover adviseren en het ondersteunen van gebruikers.
Motivering van keuze	De Technische ISO is binnen een gemeente de technische specialist op het gebied van informatiebeveiliging. Bij de invoering van nieuwe of vernieuwde systemen, de toepassing van nieuwe technologieën, procedures, maar ook als zaken in de praktijk niet goed blijken te lopen wordt de Technische ISO ingeschakeld. Daarnaast handelt de Technische ISO vragen en klachten af van gebruikers binnen de gemeente over deze systemen, en ondersteunt hen in het gebruik.
Keuze functie	**Systemen II**
	• **ontwikkelt mede** de infrastructuur • **richt** ICT-systemen, netwerken en applicaties **in en beheert deze** • ondersteunt gebruikers **bij complexe problemen**

Motivering o.b.v. overwegende functiekenmerken	De Technische ISO ontwikkelt mede de infrastructuur rondom privacy en beveiligingsrisico's (dus het risico dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van informatie wordt aangetast) en richt de ICT-systemen, netwerken en applicaties binnen de gemeente hierop in. Als specialist past de Technische ISO technologieën toe op een aanvaardbaar niveau en heeft een rol bij de ontwikkeling van nieuwe projecten/systemen. Anderzijds, onderhoudt en beheert hij bestaande systemen, applicaties en de infrastructuur.
Motivering o.b.v. resultaatgebieden	• **Resultaatgebied 1: Ontwikkeling infrastructuur** • **Resultaatgebied 2: Systeem-, netwerk- en applicatiebeheer** • **Resultaatgebied 3: Gebruikersondersteuning**
	1. Ontwikkeling infrastructuur • Afstemmen van informatiebeveiliging met lopende projecten binnen de organisatie (technische kant). • Vertalen van wensen en behoeften van gebruikers, rondom informatiebeveiliging, naar inrichting en toepassingen. • Zorgdragen voor en adviseren over de inrichting en de werking van netwerken, systemen en applicaties rondom informatiebeveiliging. • Adviseren over aan te schaffen apparatuur en programmatuur en het opstellen van een programma van eisen. • 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.
	2. Systeem-, netwerk- en applicatiebeheer • Optreden als intermediair tussen gebruikers en leveranciers. • Ontwerpen, verzorgen en bewaken van koppelingen tussen ICT systemen en applicaties rondom informatiebeveiliging. • Zorgdragen voor de technische beveiliging en autorisaties.
	3. Gebruikersondersteuning • Verzorgen en coördineren van voorlichting en interne opleidingen van het personeel op het gebied van ICT systemen en informatiebeveiliging. • Verzamelen en registreren van informatie over de aanwezige beveiligingsmaatregelen en beveiligingsincidenten. • Afhandelen van vragen en klachten van gebruikers binnen de gemeente over de ICT-infrastructuur rondom informatiebeveiliging. • Ondersteunen van gebruikers bij (nieuwe) ICT-voorzieningen en de ICTinfrastructuur rondom informatiebeveiliging, binnen de gemeente.

Vergelijking met het hogere en lagere niveau binnen de functiegroep	De naast hogere functie, Systemen I, heeft een grote rol in beleidsadvisering en het ontwikkelen van beleid, deze rol is meer weggelegd voor de Concern of Domein ISO. Systemen I is daarom niet passend. De naast lagere functie, Systemen III, draagt niet bij aan de ontwikkeling van de ICT-infrastructuur en ondersteunt gebruikers in minder complexe problemen. Systemen III is daarom niet passend.

Bijlage 2 Uitwerking competenties

e-Competenties (uit e-CF)

Het beroepsprofiel is is gebaseerd op het Europees e-Competence Framework 3.0 (e-CF). Een e-CF is een specifieke competentie (ofwel benodigde kennis) voor een IB-professional.

Toelichting op de e-Competenties[6]

D.1. Beleidsontwikkeling informatiebeveiliging:

Stelt beleid op voor een formele organisatiestrategie om de veiligheid en beveiliging van informatie tegen externe en interne dreigingen te handhaven. Met dit beleid wordt de basis gelegd voor informatiebeveiligingsbeheer, inclusief vaststellen van rollen in de beveiligingsorganisatie en hun aansprakelijkheid. Maakt gebruik van gedefinieerde standaarden om doelstellingen te creëren voor de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens.

E.3. Relatiemanagement

Implementeert het risicobeheer over informatiesystemen door toepassing van het door de organisatie gedefinieerde informatiebeveiligingbeleid en de uitwerking hiervan in een beveiligingsplan. Helpt het risico voor de bedrijfsactiviteiten van de organisatie te beoordelen, op basis van verschillende soorten dreigingen (digitaal, fysiek, organisatorisch, technisch). Legt de activiteiten om risico's te verminderen vast.

E.8. Informatiebeveiligingsmanagement

Implementeert informatiebeveiligingsbeleid. Controleert en initieert actie door de lijnmanagers tegen indringers, fraude en beveiligingslekken. Zorgt ervoor dat beveiligingsrisico's worden geanalyseerd en beheerd met betrekking tot bedrijfsgegevens en -informatie. Evalueert beveiligingsincidenten, doet aanbevelingen voor beveiligingsbeleid en -strategie om continue verbetering van de beveiliging te garanderen.

Algemene competenties

In het beroepsprofiel zijn ook competentieniveaus m.b.t. vaardigheden onderscheiden (algemene competenties). Een vaardigheid wordt afgemeten aan twee aspecten, namelijk de *complexiteit* van de betreffende activiteit en de mate van *zelfstandigheid* waarmee de professional deze activiteit uit kan voeren. Het vaardigheidsniveau geeft aan in welke mate de CISO een activiteit zelfstandig moet kunnen uitvoeren (1 = onder begeleiding; 5 = geheel zelfstandig). De algemene competenties zijn in het beroepsprofiel niet verder uitgewerkt. Het uitgangspunt is namelijk dat voor deze competenties al voldoende referentiemodellen bestaan vanuit het hrm-vakgebied.

6 Genoemde competenties zijn een vertaling van de oorspronkelijke Engelse tekst, die terug te vinden is in het genoemde e-Competence Framework.

Bijlage 3 Opleidingsaanbod

Hieronder wordt een aantal certificeringen weergegeven, die een aanvulling zouden kunnen zijn op de startkwalificatie van de CISO. Het overzicht bevat slechts een paar voorbeelden en heeft niet de intentie om uitputtend te zijn. Kenmerk van alle genoemde opleidingen is dat zij ervaring in de uitoefening van een IB-functie als uitgangspunt nemen. Om voor certificering in aanmerking te komen, geldt naast het afronden van de opleiding vaak een ervaringseis van tenminste vijf jaar.

Titel opleiding	Toelichting
CISM	Certified Information Security Manager. Deze opleiding richt zich met name op management en organisatie van informatiebeveiliging, op het niveau van leidinggevenden en eindverantwoordelijken. Certificering vindt plaats door de Information Systems Audit and Control Association (ISACA).
CISA	Certified Information Systems Auditor. Waar CISM zich richt op de managementkant, is de CISA gericht op de auditing van informatiebeveiliging. Deze opleiding wordt ook gecertificeerd door ISACA.
CISSP	Certified Information Systems Security Professional. Deze opleiding heeft een brede scope op alle verschillende domeinen van het vakgebied informatiebeveiliging, zowel de technische als de organisatorische aspecten. Dit vereist een brede voorkennis van het vakgebied. Certificering vindt plaats door het International Information System Security Certification Consortium (ISC2).
CRISC	Certified in Risk and Information Systems Control. Deze opleiding richt zich met name op de beheersing van risico's in het kader van informatiebeveiliging. Certificering vindt plaats door ISACA.
C|CISO	Certified Chief Information Security Officer. Deze opleiding is een programma van de EC-Counsil, samengesteld door ervaren CISO’s over de hele wereld. Het test de praktische kennis op een vijftal domeinen, waarbinnen kandidaten tenminste vijf jaar werkervaring hebben opgedaan. Deze ervaring geldt als toelatingsdrempel voor het examen dat tot de certificering tot CCISO leidt.

Bijlage 4 Geraadpleegde literatuur

- European ICT professionals role profiles (CWA16458), part 1: 30 ICT Profiles, CEN (European committee for standardization), 2018;
- European e-Competence Framework 3.0, A common European Framework for ICT Professionals in all industry sectors. CWA 16234:2014 Part 1. © CEN;
- Het inrichten van een beveiligingsorganisatie. Welke factoren zijn van invloed?, GvIB Expert Brief – Juli 2006;
- Functies en rollen in de informatiebeveiliging, GvIB Expert Brief - Maart 2005;
- Beroepsprofielen Informatiebeveiliging 2.0, QIS/PvIB, januari 2017;
- Onderzoek naar kwalificatie en certificatie van informatiebeveiligers, Marcel Spruit/Fred van Noord, 2011.
- Durven leren. Eindrapport van de Visitatiecommissie Informatieveiligheid, september 2017.

INFORMATIE
BEVEILIGINGS
DIENST

Kijk voor meer informatie op:
www.informatiebeveiligingsdienst.nl

Nassaulaan 12
2514 JS Den Haag
CERT: 070 373 80 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)
info@IBDGemeenten.nl / incident@IBDGemeenten.nl

VNG Realisatie