Enquête
CISO's
binnen de Nederlandse overheid

Hoe ervaren CISO's hun werk en werkomgeving?

Een onderzoek naar de invulling van de functie van Chief Information Security Officers binnen de overheid vanuit het perspectief van CISO's én betrokken bestuurders.

Amsterdam, 21 oktober 2019

Colofon

Deze enquête is tot stand gekomen op initiatief van CIP, met medewerking van een aantal CISO's, werkzaam bij het rijk, gemeenten, waterschappen, uitvoeringsorganisaties, Hoge Colleges van Staat en het NCSC. De vragenlijsten zijn ontwikkeld en verwerkt door het CIP, tevens verantwoordelijk voor de analyse en het opstellen van dit rapport.

Amsterdam, september/oktober 2019

1 Inhoud

2 Inleiding/aanleiding

Het beroep van Chief Information Security Officer (CISO) bestaat zo'n twintig jaar. Maar het beroep of de rol is niet wettelijk beschreven, noch verplicht en heeft ook geen beschermde status. Algemene eisen waaraan de CISO moet voldoen, zijn nergens vastgelegd.

Om na te gaan hoe de invulling van de functie van CISO (binnen de Nederlandse overheid) in de praktijk gestalte krijgt en hoe CISO's hun werk en werkomgeving ervaren, heeft CIP in 2019 een enquête uitgezet. CIP hoopt dat de uitkomsten van de enquête kunnen bijdragen aan het formuleren van nadere eisen aan het beroep, nadere input kunnen opleveren voor opleidings- en inbeddingscriteria en steun kunnen geven aan de praktische invulling van de functie. Naast de enquête onder CISO's zijn separaat ook vragen voorgelegd aan bestuurders over hun visie op de rol van en samenwerking met de CISO. Parallel aan het enquêtetraject is CIP onlangs gestart met het organiseren en inrichten van een community van CISO's binnen de overheid. De uitkomsten van de enquête worden hierin meegenomen.

Dit document bevat een analyse van de antwoorden die CISO's en bestuurders in september 2019 hebben gegeven op de vragen in de betreffende enquêtes. Een samenvatting van de uitkomsten staat beschreven onder hoofdstuk 3.

We zijn veel dank verschuldigd aan allen die hebben meegedaan. De substantiële respons draagt in hoge mate bij aan de relevantie van de uitkomsten. Ruim 100 CISO's en bijna 40 bestuurders hebben de enquêtes volledig ingevuld. Invullingen van open vragen en overige opmerkingen en suggesties zijn gebruikt als achtergrond bij de analyse en in sommige gevallen ook getoond in de bijlagen.

Over CIP

CIP is het Centrum voor informatiebeveiliging en privacybescherming van, voor en door overheidsorganisaties. Het heeft zich ontwikkeld tot een publiek-private netwerkorganisatie, waaraan ook gespecialiseerde marktorganisaties als kennispartners deelnemen.

Het centrum is opgericht voor informatie-uitwisseling en kennisdeling ter verbetering van de informatieveiligheid van de overheidsdienstverlening. Inmiddels bestaat het CIP-netwerk uit een groot aantal overheidsorganisaties en (private) kennispartners. De aanwezige kennis op het gebied van informatiebeveiliging en privacybescherming wordt binnen de samenwerking in CIP-verband op verschillende manieren gedeeld en toegankelijk gemaakt. Deze samenwerking draagt bij aan het optimaal gebruik van overheidsmiddelen.

3 Samenvatting en aandachtspunten

Ondanks het gegeven dat de gemiddelde leeftijd van de CISO 55 jaar bedraagt, is de ervaring in de functie van CISO relatief kort. 40% geeft aan slechts 0 tot 2 jaar werkervaring te hebben en nog eens 40% 3 tot 5 jaar.

Veel CISO's rapporteren aan een bestuurder of directeur. Uit het oogpunt van risicomanagement en toezicht heeft het grote voordelen dat de CISO een neutrale positie inneemt t.o.v. de verantwoordelijke voor informatievoorziening en ICT. Het onderzoek laat zien dat deze rapportagelijn binnen veel organisaties al gangbaar is. Tegelijkertijd is het een aanmoediging om deze werkwijze door te voeren daar waar de CISO nu nog rapporteert aan de CIO en onderdeel is van de ICT/CIO-organisatie.

Over de beschikbare capaciteit van CISO's is het beeld niet positief. Voor 69% van de CISO's betreft het een parttime functie. 77% heeft geen team of medewerkers. 40% heeft geen budget (22% een heel klein budget). Dit komt de status en slagvaardigheid van deze 'solistische' functie niet ten goede. Aangeraden wordt de CISO te voorzien van een eigen budget. Dit kan zijn effectiviteit ten goede komen, het zelfstandig handelen bevorderen en de zelfstandige positie in de organisatie helpen verstevigen. Kortom, meer armslag én een steun in de rug voor deze taaie 'gewetensrol'!

Taakopvattingen omtrent rol van de CISO bij henzelf en bij de bestuurders zijn behoorlijk congruent. Daarbij valt op dat een rol voor de CISO bij inkopen en aanbestedingen nauwelijks wordt gezien. Dit blijkt ook uit een vraagstelling over de eisen die meegegeven worden aan leveranciers. Die blijken zeer algemeen van aard. Hier ligt een urgent verbeterpunt in organisaties en een stevige taak voor de CISO. Hulp is inmiddels onderweg, want het ministerie van BZK ontwikkelt samen met CIP en een interbestuurlijke expertgroep, tooling om bij inkopen passende eisen op het gebied van informatiebeveiliging (IB) te kunnen selecteren.

Het is opvallend dat CISO's meer bewustwording over IB-risico's willen zien bij hun bestuurders, terwijl de risicoperceptie bij bestuurders in het algemeen zelfs hoger ligt dan bij de CISO's zelf. Meer frequent onderling overleg kan zorgen voor een betere afstemming tussen beide partijen.

In 43% van de gevallen is de CISO niet of alleen incidenteel betrokken bij IV-veranderingen. Het is daarom van belang dat de CISO op structurele basis betrokken is bij de veranderingsprocessen in de informatievoorziening. Informatieveiligheid is namelijk een steeds dominanter kwaliteitsaspect en moet als integraal onderdeel worden meegenomen en geborgd.

Desgevraagd geven de responderende CISO's aan slechts in beperkte mate zicht te hebben op de omvang of het effect van IB-gerelateerde schade bij incidenten. 70% geeft te kennen daarop onvoldoende (45%), of zelfs helemaal geen zicht (25%) te hebben. Zijn er te weinig harde gegevens bekend bij de CISO's uit risicoanalyses? Harde conclusies zijn niet mogelijk. Maar aangezien ook de Baseline Informatiebeveiliging Overheid (BIO) risicoanalyses veronderstellen, is dit op zijn minst een aandachtspunt.

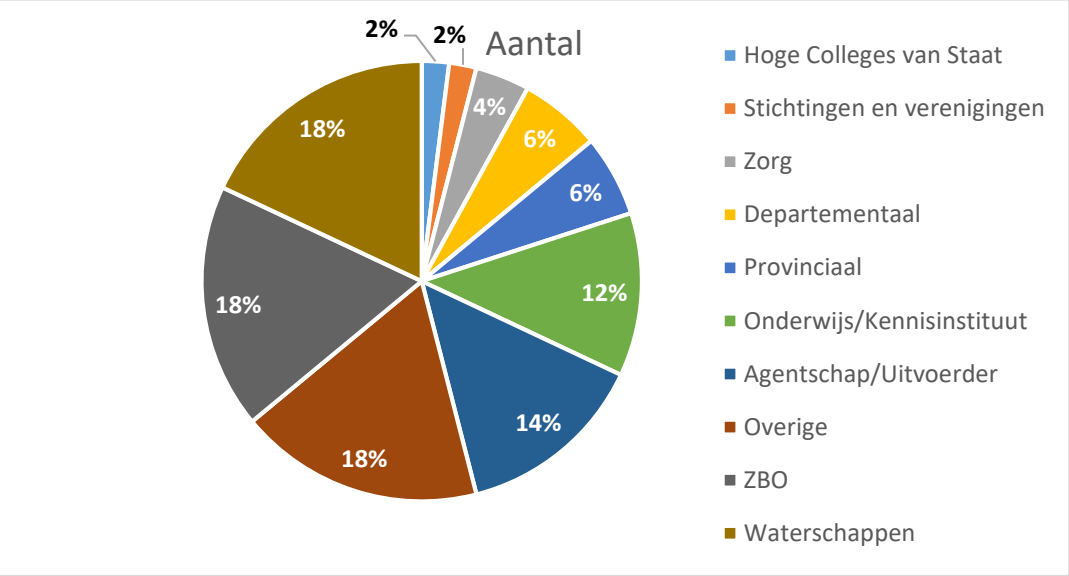
92% van de organisaties voert *hack-/pentests* uit. *Phishing* campagnes komt in 62% van de organisaties voor, *mystery guests* in 48% en periodieke crisisoefeningen in 30% van de organisaties. Oefeningen zijn vaak niet structureel ingebed. CIP adviseert om hier periodiek aandacht aan te besteden. Dit helpt organisaties veilig te houden en zorgt ervoor dat signalering en response op incidenten structureel geborgd is.

Aansluitingen op het Nationaal Detectie Netwerk (NDN) zijn schaars. Het is aan te raden om het NDN toegankelijk te maken voor de gehele overheid. Dit kan een verbetering tot stand brengen in de signalering van cyberdreigingen. Ook Information Sharing & Analysis Centers (ISAC'S), kennen weinig deelname en uitstraling naar buiten. Veel kleinere organisaties blijven hierdoor verstoken van nuttige informatie over kwetsbaarheden en incidenten en hoe daarmee om te gaan. Ook de relatieve onbekendheid (onder CISO's) van dit soort organisaties is een opvallende enquête-uitkomst. Het op neutrale wijze breder uitdragen van de uitwisselingen binnen de ISAC's kan een oplossing zijn voor diegenen die niet kunnen deelnemen aan een ISAC. CIP kan hier t.g.t. een rol in spelen in samenwerking met het Nationaal Cyber Security Centrum (NCSC).

4 Profiel van de respondenten

4.1 Welke sectoren

CISO-Enquête
De CISO Enquête is uitgezet in het CIP-netwerk en is voornamelijk ingevuld door CISO's uit de verschillende overheidslagen. De helft van de respondenten betreft gemeentelijke CISO's. Zie voor de herkomst van de overige respondenten onderstaand diagram.



Organisaties geteld in de sector 'Overige', zijn onder meer een veiligheidsregio, omgevingsdienst, toezichthouder, een shared service center, een organisatie actief in het sociaal domein en een energie-transporteur.

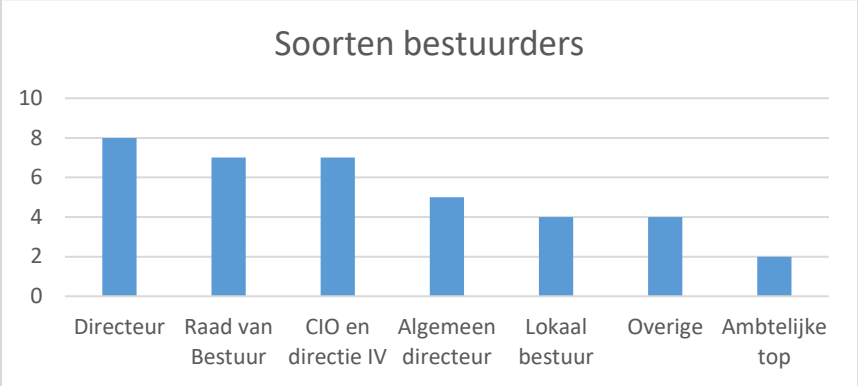
Bij de verdere analyse in dit document richten we ons vooral op de groep als totaal. Daarnaast wordt, waar relevante verschillen optreden, onderscheid gemaakt tussen de groepen gemeentelijk - niet gemeentelijk.

Mini-enquête bestuurders
De specifiek op bestuurders gerichte mini-enquête is ingevuld door mensen uit dezelfde sectoren, maar in een andere verhouding:

- 39% betreft respondenten uit ZBO's, andere uitvoerders en agentschappen,
- 24% uit gemeenten,
- 15% departementaal,
- 10% uit provincies en waterschappen en
- 12% uit overige overheidsorganisaties.

De achtergrond wat betreft functie en titel is bij de bestuurder divers. De meesten van hen hebben geen vakinhoudelijke-, maar een algemene verantwoordelijkheid. Het betreft de hoogste leidinggevenden die door hun eigen CISO voor deelname aan deze enquête zijn uitgenodigd, dan wel direct door CIP. Dit zijn functionarissen die het beeld vanuit de andere kant van de tafel kunnen belichten, conform het doel van deze deelenquête.

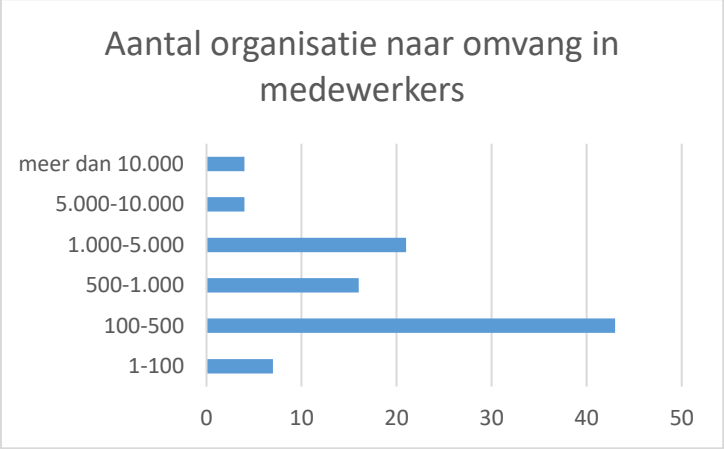
Onderstaande grafiek geeft aan welke typen functionarissen deelnamen aan de bestuurdersenquête.



4.2 Omvang van de organisaties

Onderstaand diagram toont dat meer dan de helft van de respondenten uit organisaties van beperkte omvang (<500) afkomstig is, gemeten naar het aantal werknemers/fte's. (Dit geldt zowel voor de CISO's als voor de bestuurders). Dat is niet verwonderlijk gelet op het grote aantal respondenten werkzaam bij gemeenten, waaronder relatief veel kleinere organisaties die binnen de overheid voorkomen.

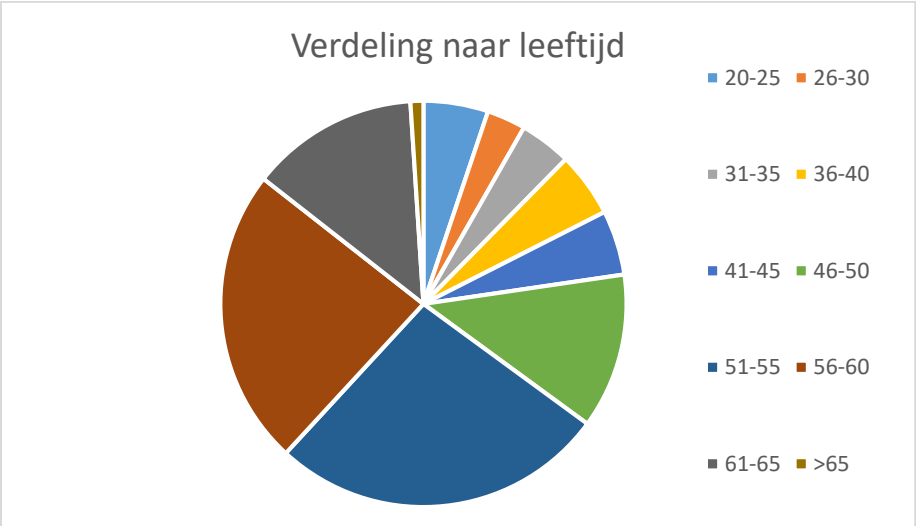
In het volgende diagram staat de verdeling van respondenten over grotere en kleinere organisaties.



5 Profiel van de CISO

5.1 Leeftijdsopbouw

De gemiddelde leeftijd van de CISO's in dit onderzoek is ca. 55 jaar. De grootste groep bevindt zich in de leeftijd van 51 tot 60 jaar. Onderstaand grafiek toont de verdeling van de leeftijdsgroepen.

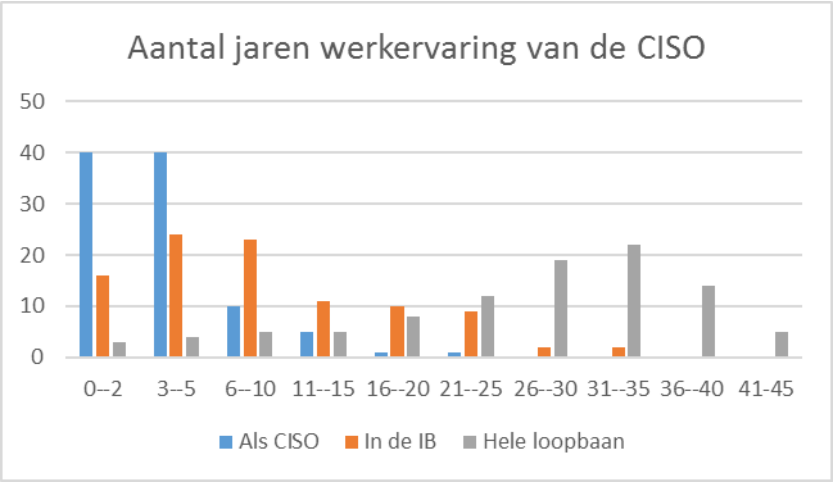


5.2 Jaren werkervaring

Het merendeel van de CISO’s heeft een forse werkervaring. Verreweg het grootste deel (ca. 75%) heeft meer dan 20 jaren werkervaring. Dit correspondeert met de leeftijdsopbouw.

Veel van de CISO’s zijn ook al langere tijd in het vakgebied van de informatiebeveiliging werkzaam (60% langer dan 6 jaar).

Het is anders gesteld met de ervaring in de CISO-functie zelf. Van alle CISO’s in dit onderzoek geeft 40% aan slechts 0 tot 2 jaar werkervaring te hebben en nog eens 40% 3 tot 5 jaar. Langjarige ervaring in deze functie c.q. rol is schaars. Opvallend is dat dit beeld niet relevant verschilt tussen grote en kleine organisaties.



5.3 Opleidingen

Niveau
De respondenten hebben opgegeven te beschikken over de volgende opleidingsniveaus:

- Academisch niveau: 48%.
- Hbo niveau: 43%.
- Mbo niveau of lager: 9%.

Vakopleidingen
In een open vraag konden de respondenten hun specifieke, vakgerichte opleidingen vermelden. Vrijwel alle respondenten geven aan aanvullende opleidingen te hebben gevolgd. Het gaat dan om een grote verscheidenheid aan cursussen, in-huis-opleidingen van de eigen organisatie, trainingen van gespecialiseerde bedrijven, etc.

Vaak genoemd werden:

- CISM – 18 keer
- CISSP – 16 keer
- Diverse CISO masterclasses en cursussen – 15 keer
- CISA – 6 keer en
- CIPP/E – 4 keer

12% meldt andere dan IB-specifieke opleidingen te hebben gevolgd, terwijl 9% te kennen geeft geen enkele vakinhoudelijke vakopleiding te hebben gevolgd.

In Bijlage II is de volledige lijst van genoemde opleidingen en cursussen opgenomen.

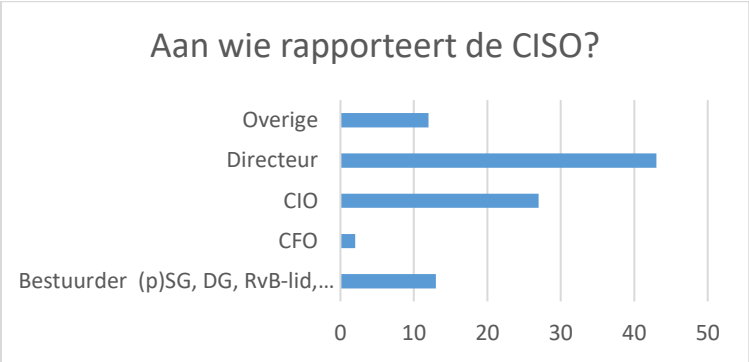
6 Functie-invulling en CISO-organisatie

6.1 Rapportagelijnen

De CISO's die meededen aan de enquête blijken in veel gevallen (68%) te rapporteren aan een directeur of bestuurder. In 32% van de gevallen wordt gerapporteerd aan de CIO of een andere inhoudelijke manager.

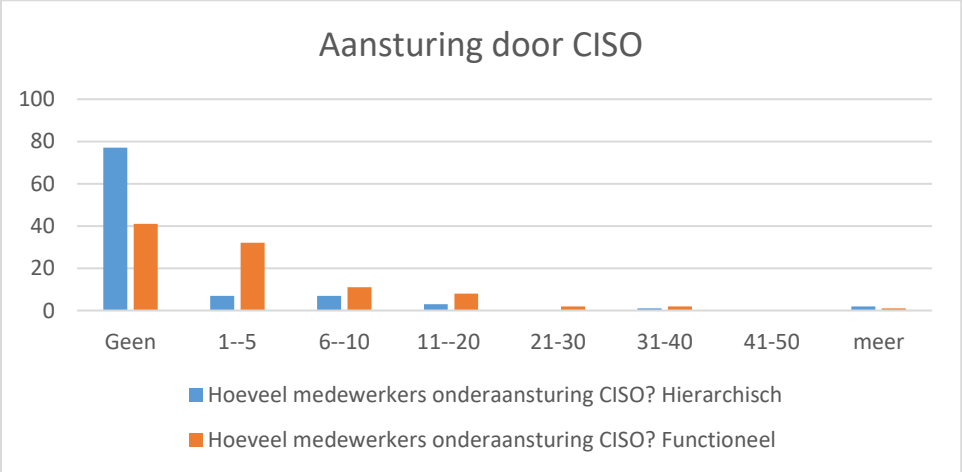
Uit het oogpunt van risicomanagement en toezicht heeft het grote voordelen dat de CISO een neutrale positie inneemt t.o.v. de verantwoordelijke voor informatievoorziening en ICT.

Het onderzoek laat zien dat deze rapportagelijn binnen veel organisaties al gangbaar is. Tegelijkertijd is het een aanmoediging om deze werkwijze door te voeren daar waar de CISO nu nog rapporteert aan de CIO en onderdeel is van de ICT/CIO-organisatie.



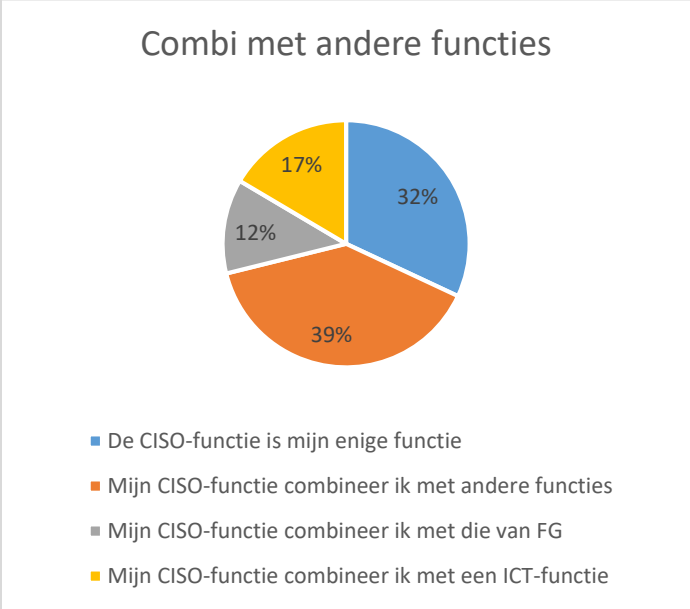
6.2 Aansturing

Van de deelnemende CISO's aan deze enquête zegt 77% geen enkele andere medewerker op het domein van informatiebeveiliging hiërarchisch aan te sturen. Slechts 23% heeft één of meer medewerkers 'onder zich'. De hoogste verantwoordelijke voor dit domein heeft een eenzame centrale functie. Helemaal als dit wordt gecombineerd met 41% die ook nog eens geen enkele decentrale medewerker functioneel aanstuurt. De conclusie luidt dat voor 41% van alle respondenten de CISO-functie een solistische job is.



6.3 Combinatie met andere functies

In combinatie met het voorgaande is het opvallend dat de CISO-functie vaak een parttime functie betreft: 69% heeft daarnaast ook nog een andere functie. Van de 40% die 2 jaar of minder CISO-ervaring heeft, is het aandeel parttime CISO's 75%. Dat roept de vraag op of de functie wel voldoende prioriteit krijgt.



In 12% van de gevallen geeft men aan dat het gaat om de combinatie met de functie van Functionaris Gegevensbescherming. Deze combinatie heeft in ieder geval inhoudelijke synergie. De combinatie met een ICT-functie (16%) kan problemen opleveren vanuit risk management optiek.

De combinatiefuncties die men opgeeft bij 'Overige' is een variëteit van ICT-, Privacy-, Risk- en planning & control-functies. Ook de combinatie met ENSIA-coördinator (een functie die alleen bij gemeenten voorkomt) komt meerdere keren voor.

Apart werd de vraag gesteld naar de combinaties met de verantwoordelijkheid voor integrale veiligheid. Dit is ook een natuurlijke, synergetische combinatie. Deze combinatie komt slechts voor in 13% van de situaties.

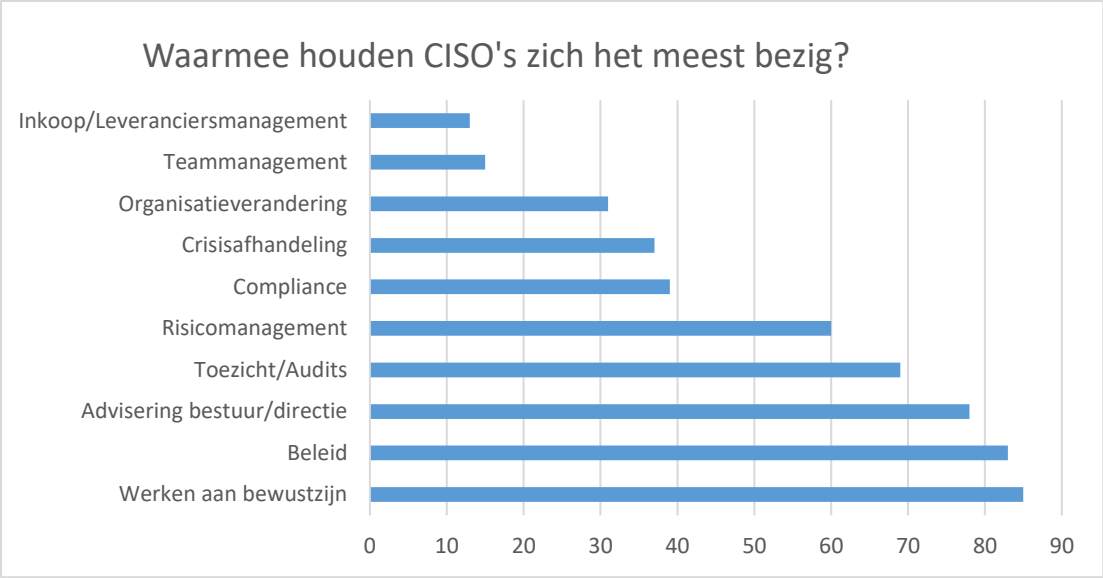
6.4 Taakgebieden

De CISO's geven aan dat hun belangrijkste taken liggen op het gebied van het verbeteren van beleid, het adviseren van de directie/bestuurders en het werken aan bewustzijn.

In toelichtende opmerkingen worden daarbij nog onderwerpen genoemd als: achterstanden wegwerken, cultuur, implementatie, IB architectuur, privacy, business continuïteit, richtlijnen en externe overleggen.

Regelmatig worden genoemd: veel te veel operationeel werk en te weinig strategisch bezig kunnen zijn.

De vraag naar de belangrijkste taken van de CISO werd ook aan bestuurders gesteld. De beelden van de CISO's en de bestuurders over de taakinvulling blijkt behoorlijk congruent, zoals te zien is in onderstaande diagrammen.



Gezien het belang van informatieveiligheid van inkopen/aanbestedingen is het wel opmerkelijk dat de CISO nauwelijks betrokken is bij inkopen en leveranciersmanagement. Dit punt komt verder ter sprake in paragraaf 8.6.

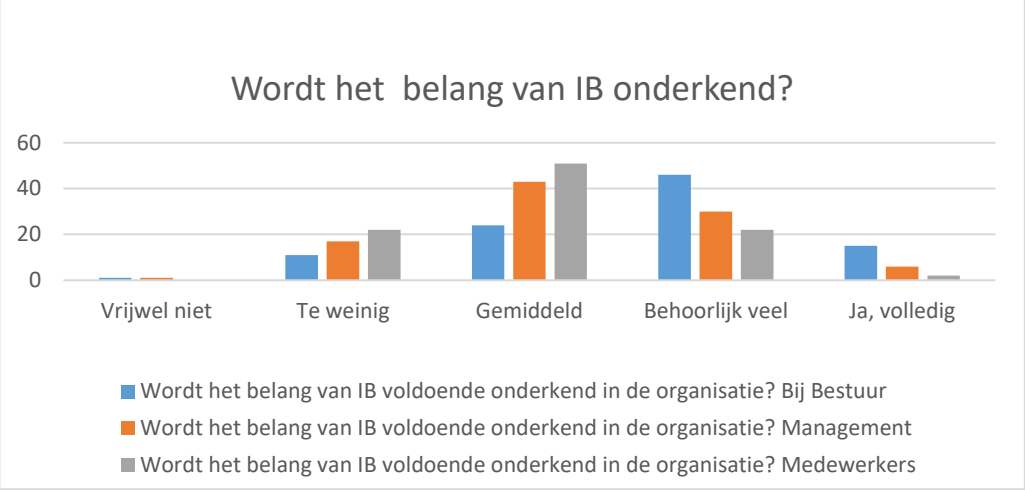
Omdat de gemiddelde CISO uit het onderzoek nauwelijks mensen aanstuurt, is de lage prioriteit die wordt toegekend aan 'teammanagement' niet verwonderlijk. Maar omdat verantwoord gedrag op de werkvloer (wat op 'bewustzijn' zou moeten volgen) wel belangrijk wordt geacht door CISO's én bestuurders, is de lage prioriteit die aan organisatieverandering wordt toegekend wel opvallend (zie ook paragraaf 7.1 'Draagvlak en begrip' op de volgende pagina).

7 Conditionering van de CISO

7.1 Draagvlak en begrip

Informatieveiligheid is onderdeel van de lijnverantwoordelijkheid. Vandaar de vraagstelling naar draagvlak en begrip op de diverse niveaus binnen die lijn. Zonder dat dit draagvlak en begrip op niveau zijn, lijdt informatieveiligheid een zieltogend bestaan.

In tegenstelling tot signalen die regelmatig binnen ons netwerk klinken zeggen de deelnemende CISO's dat het over het algemeen niet ontbreekt aan ondersteuning van de bestuurders. Wel is er binnen diverse organisaties ruimte voor verbetering. Met de ondersteuning van (middel-) management en het begrip bij medewerkers is de situatie minder rooskleurig. De vertaling van het belang van informatieveiligheid door de top naar alle managementlagen binnen de organisatie verdient aandacht.



Wat CISO's vooral van bestuurders vragen is interesse, betrokkenheid en steun, commitment m.b.t. informatieveiligheid, zelf een voorbeeldfunctie vervullen en actief als ambassadeur het belang ervan uitdragen. Zie bijlagen III, IV, V en VI, voor wat CISO's en bestuurders hebben gezegd over hun rollen en verbetermogelijkheden.

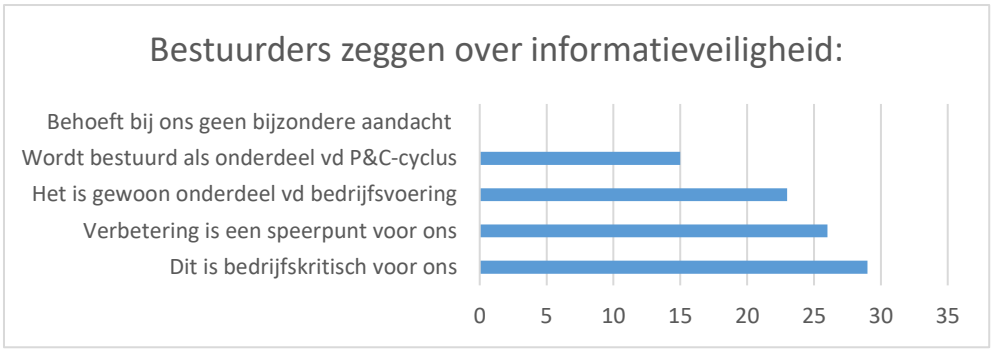
Hoewel een ruim aantal CISO's aangeeft tevreden te zijn met de bestuurdersrelatie, worden ook een aantal verbeterpunten aangedragen. Met name op het gebied van bewustwording t.a.v. de IB-risico's bij bestuurders en de behoefte om meer frequent overleg te hebben met de bestuurder.

Hierbij is het opvallend dat de risicoperceptie bij bestuurders in het algemeen aanmerkelijk hoger ligt dan bij de CISO's zelf (zie par. 9.1). Bestuurders vragen ook om een meer adviserende rol van de CISO's. Meer frequent overleg is te adviseren om de beelden op elkaar af te stemmen.

7.2 Wat zegt de bestuurder over het belang van informatieveiligheid?

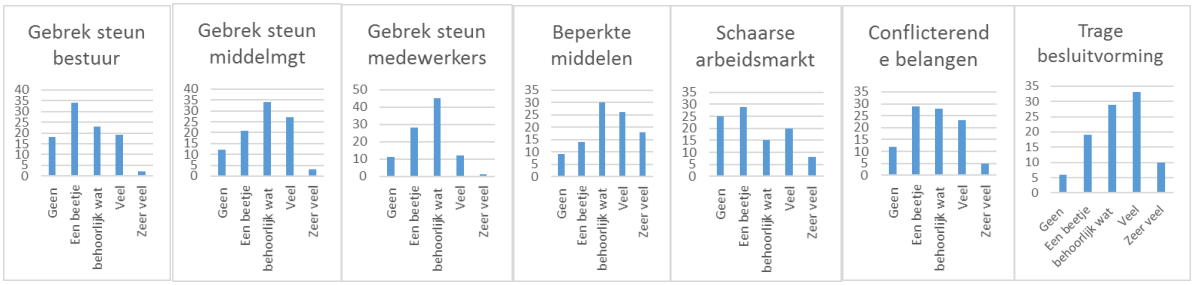
Bestuurders zijn van het belang van informatieveiligheid overtuigd. Niemand zegt dat het thema geen bijzondere aandacht nodig heeft. 76% van hen vindt informatieveiligheid van bedrijfs-kritisch belang en 68% ziet verbetering ervan als een speerpunt. Uit de invullingen is daarnaast op te maken dat de besturing onderdeel is/moet zijn van de normale bedrijfsvoering dan wel van de planning & control cyclus.

Het beeld van een gecommitteerd bestuur bevestigt het beeld dat de CISO's hierover geven. Opname van de besturing in de normale bedrijfsvoering is een goede stap in de borging van informatieveiligheid in de organisatie en een aanrader voor organisaties waar dit nog niet gebeurt

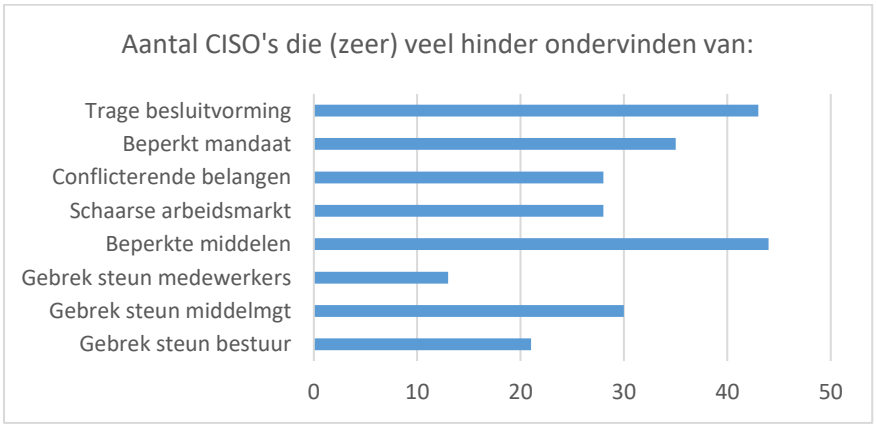


7.3 Waarvan ondervinden CISO's hinder bij hun functie-uitvoering?

Deze vraag kan worden gezien als een aanscherping van de voorgaande vraag naar de perceptie van het belang van Informatieveiligheid. De beantwoording wordt getoond in de volgende diagrammen.



Lichten we de scores op 'veel hinder' en 'zeer veel hinder' eruit, dan wordt dit het beeld:



Enkele observaties:

- Hoewel bestuurders het belang van informatieveiligheid onderkennen en CISO's dit ook bij hen hérkennen, wordt in een aantal gevallen door CISO's toch hinder ervaren van het gebrek aan steun. Vermoedelijk speelt hier mee de spanning tussen woord en daad enerzijds, en anderzijds dat de 'voice at the top' zwaar doorweegt en grote uitstraling heeft (zowel positief als negatief).
- Gebrek aan 'steun middelmanagement', 'beperkt mandaat', 'trage besluitvorming' en 'beperkte middelen' komen naar voren als grootste belemmeringen.

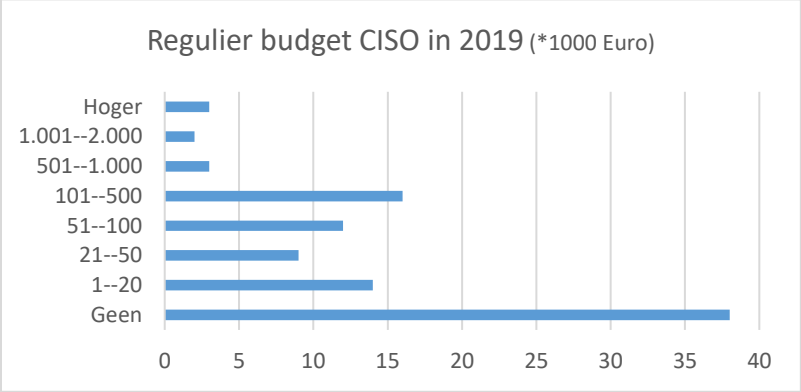
7.4 Budgetten

In de enquête werd gevraagd naar het budget waarover de CISO kan beschikken (regulier budget, projectbudget en budget in de lijnorganisatie). Onderstaand diagram geeft een beeld van reguliere budgetten in 2019.

Zo'n 40% van de CISO's beschikt niet over budget. Van het merendeel dat wel budget opgeeft is dat zeer beperkt in omvang. Er zijn wel enkele uitschieters. Het niet hebben van budget wordt in de meeste gevallen niet gecompenseerd met projectbudget. Sommigen geven aan een klein projectbudget te hebben, maar dit ligt sowieso aanmerkelijk lager dan het al schaars toegewezen reguliere budget.

In het licht van de vorige vraag, waarin veel hinder wordt gemeld van beperkte budgetten, raden we organisaties aan om bewust een budget toe te wijzen aan de CISO. Het kan de effectiviteit ten goede komen, het zelfstandig handelen bevorderen en de zelfstandige positie in de organisatie helpen verstevigen. Kortom, meer armslag én een steun in de rug van voor deze taaie 'gewetensrol'!

(NB. Op dit moment is de verwachting voor 2020 grotendeels gelijk aan 2019).



8 Stand van zaken informatieveiligheid in de organisatie

8.1 Informatieveiligheid in het jaarverslag

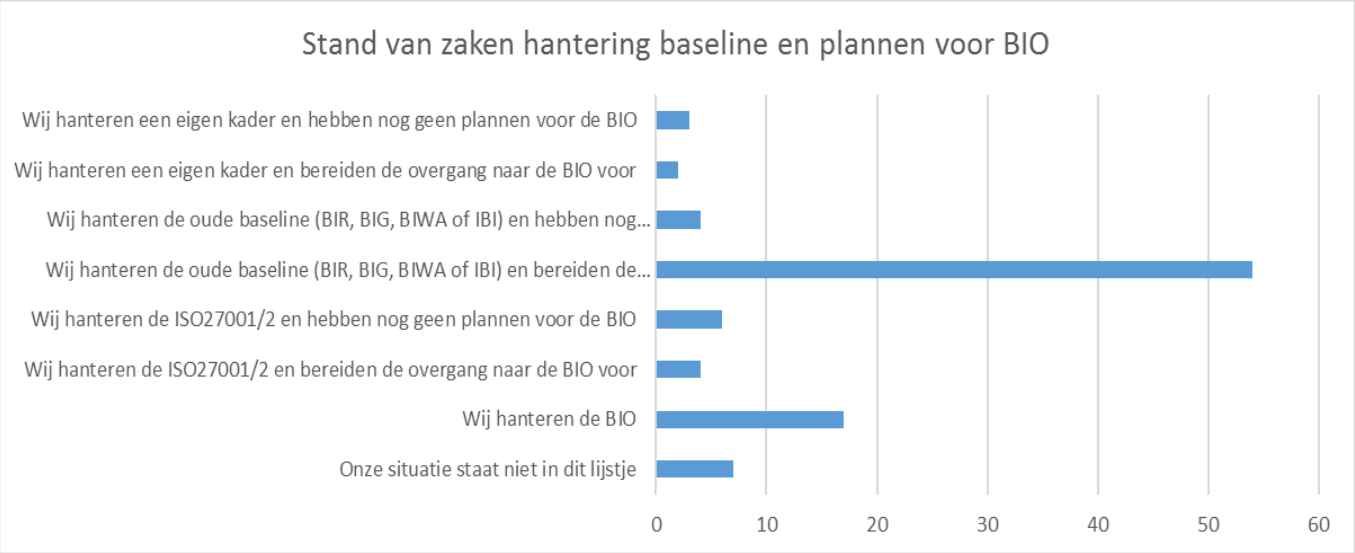
In de meeste gevallen wordt over Informatiebeveiliging gerapporteerd in het jaarverslag en speelt de CISO daarbij een belangrijke rol. 53% schrijft de paragraaf in het jaarverslag, 35% levert er input voor aan.

8.2 Stand van zaken van de hantering van de Baseline

Sinds januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. 2019 is een overgangsjaar. M.i.v. 2020 is het bedoeling dat alle overheidsorganisaties deze baseline hanteren. In de enquête vroegen wij naar de stand van zaken en de plannen.

Op dit moment blijkt 17% van de responderende organisaties de BIO al te hanteren. 62% van de organisaties bereidt de overgang naar de BIO voor. De meeste van deze organisaties hanteren op dit moment de voorloper (BIR, BIG, BIWA of IBI) en enkele organisatie ook nog de ISO27001/2.

19% heeft (nog) geen plannen voor de BIO. Er valt dus nog wat te stimuleren.

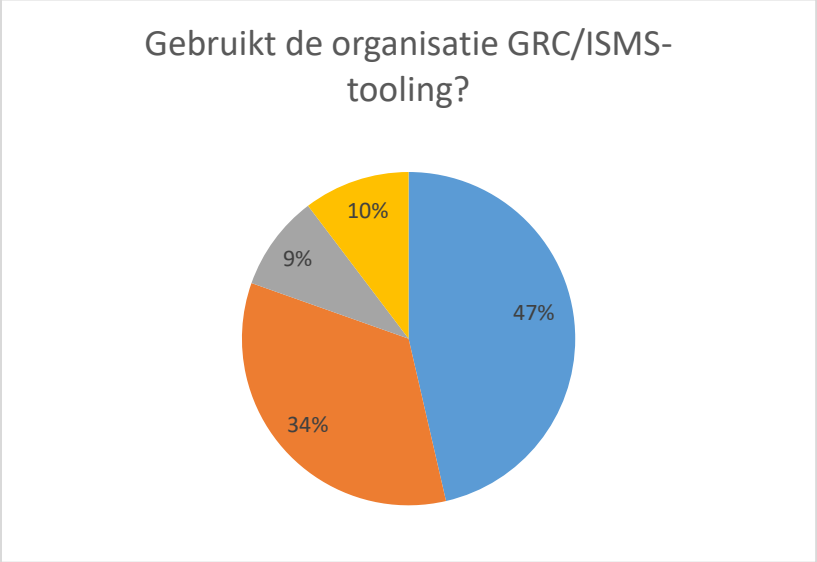


8.3 Certificering

Aan certificering blijkt op dit moment weinig behoefte. Slechts een zeer klein percentage overheidsorganisaties (3%) beschikt over een relevante certificering m.b.t. informatiebeveiliging en 14% streeft ernaar. Het gaat dan vooral om ISO 27001. De anderen hebben daaraan geen behoefte (75%) of weten het niet (8%).

8.4 Gebruik van GRC- en of ISMS-tooling

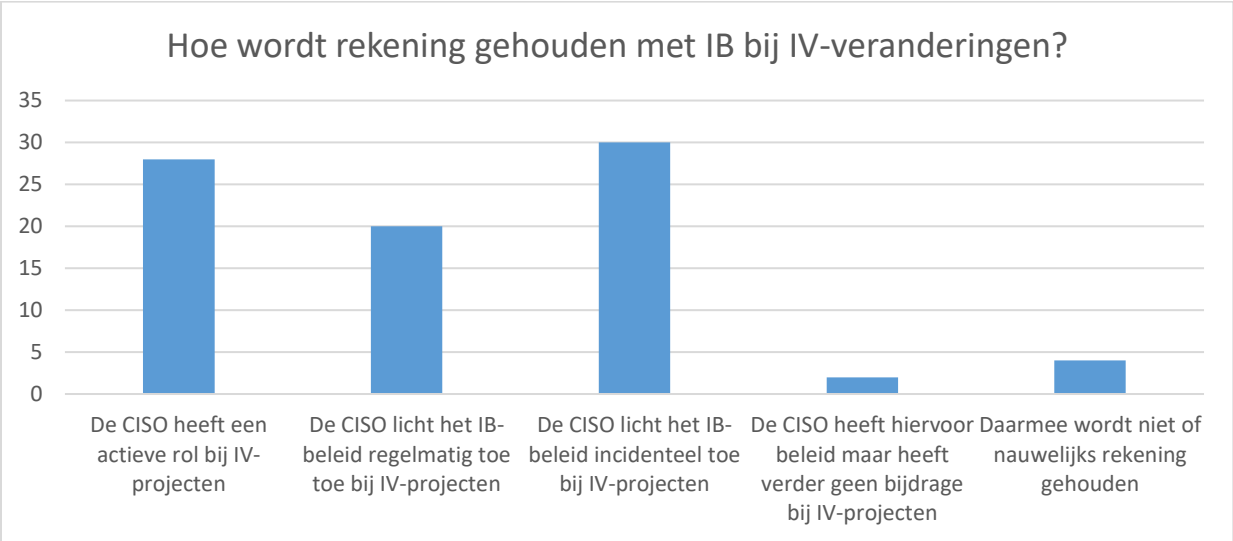
Bijna de helft van de organisaties gebruikt tooling (46%). 34% nog niet, maar gaat het wel doen. Als meest genoemde tools worden genoemd: IC Content, Key2Control, SEP, Recourse en Scienta.



8.5 Rol van de CISO bij veranderingen in de Informatievoorziening

De CISO als hoofdverantwoordelijke voor informatiebeveiliging moet een invloedrijke rol kunnen spelen bij de ontwikkeling van informatievoorziening. 57% van de ondervraagde CISO's geven aan dat dit inderdaad zo is. In 43% van de gevallen is sprake van incidentele betrokkenheid of geen betrokkenheid.

Het is van belang dat de CISO op structurele basis betrokken is bij de veranderingsprocessen in de informatievoorziening. Informatieveiligheid is namelijk een steeds dominanter kwaliteitsaspect en moet als integraal onderdeel worden meegenomen en geborgd.



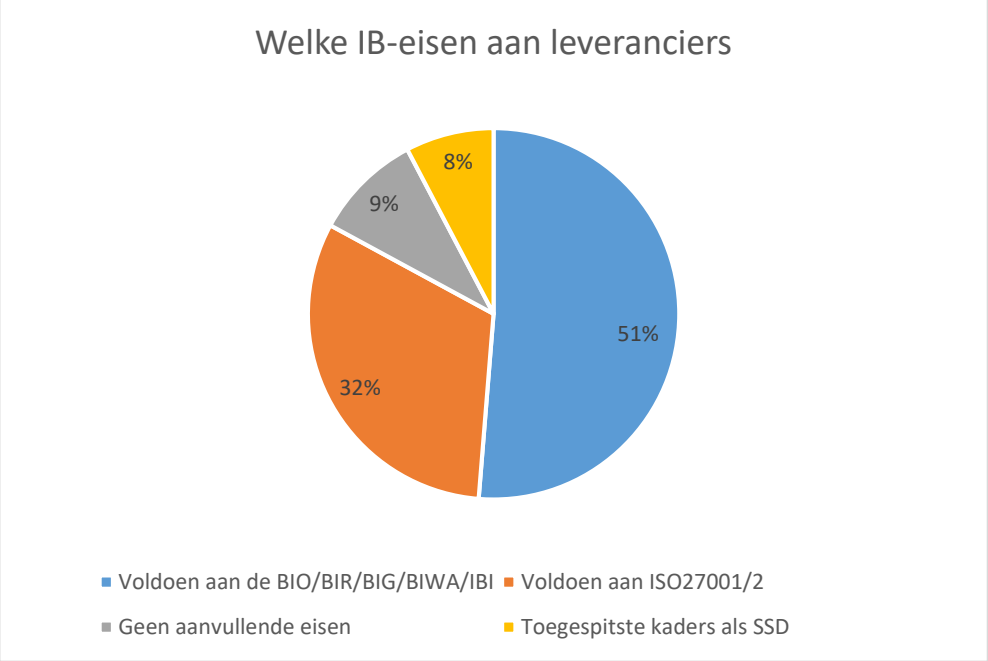
8.6 Eisen aan Leveranciers

In de enquête stelden we ook de vraag welke eisen er bovenop de algemene voorwaarden worden gesteld aan leveranciers op het gebied van informatieveiligheid.

De beantwoording is hier zeer uitgesproken. 83% geeft aan een van de baselines of ISO 27002 op te leggen en 9% hanteert geen aanvullende eisen.

Slechts 8% geeft aan specifieke eisen, zoals SSD, af te dwingen. Voorbeelden die daar vervolgens bij worden genoemd zijn richtlijnen van NCSC en CIP, zoals toepassing van Grip op Secure Software Development (SSD) en Security Proof Inkopen.

Ook Gibit wordt enkele keren genoemd. Maar dit is een kader van algemeen-juridische aard.



Opmerkelijk is het aantal keer dat de baselines worden genoemd.

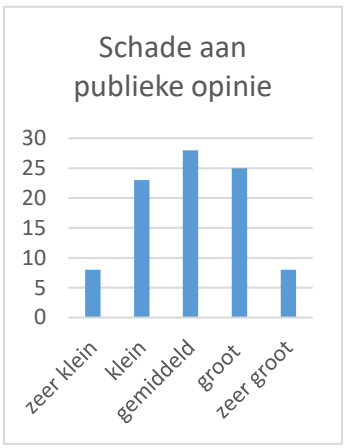
Om de veiligheid van inkopen goed te borgen is het nodig om eisen te stellen die specifiek van toepassing zijn op de scope van de inkoop. De Baselines zijn hiervoor niet geschikt. Die zijn te breed en te algemeen om te hanteren voor specifieke inkopen.

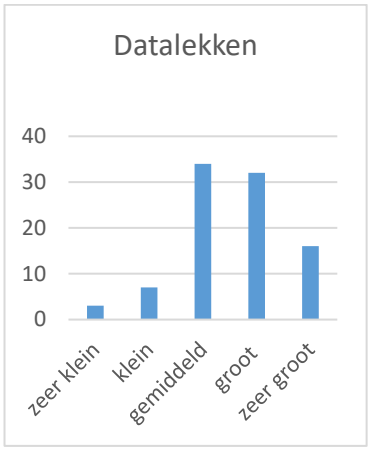
In het traject Inkoopeisen Cybersecurity Overheid (ICO) hebben het ministerie van BZK en CIP de handen ineen geslagen, met steun van een interbestuurlijke werkgroep, om tooling te ontwikkelen die kan helpen met het selecteren van scherpere eisen bij specifieke inkopen. Een prototype kan worden gedownload via cip.pleio.nl.

9 Feitelijk veiligheid

9.1 Verwachte schade

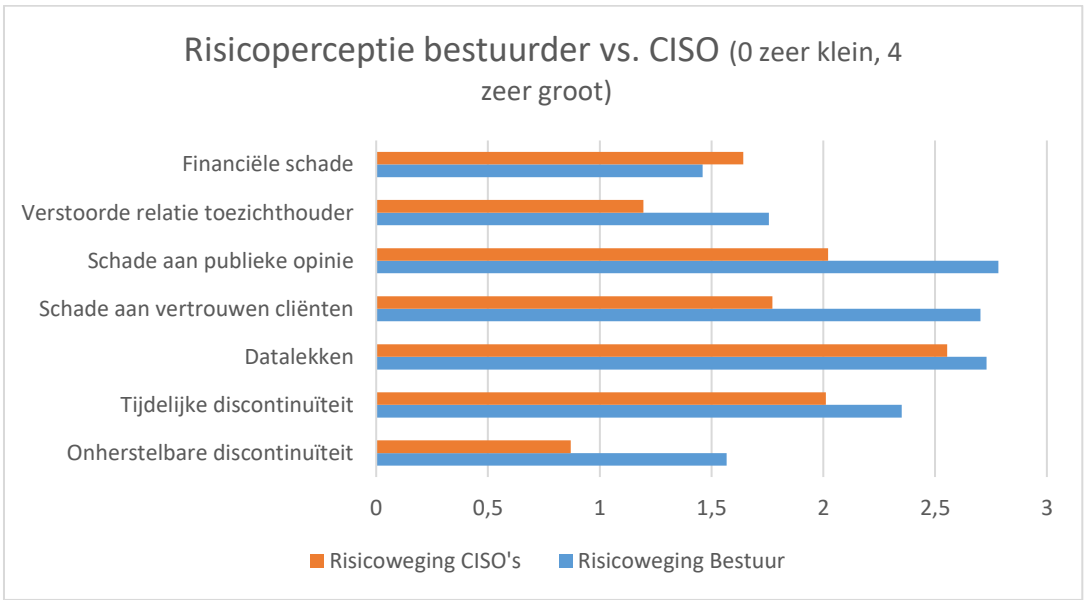
De responderende CISO's laten op het gebied van het inschatten van risico's op verschillende onderwerpen uiteenlopende scores zien. Zo wordt het gevaar op onherstelbare discontinuïteit laag ingeschat, evenals een verstoorde relatie met de toezichthouder. Meer beducht is de overheids-CISO voor tijdelijke discontinuïteit, financiële schade en beschadigd cliëntenvertrouwen. Maar de grootste zorg heeft men, zo blijkt uit de enquête, voor mogelijke schade aan de publieke opinie en vooral voor datalekken. Of deze laatste twee met elkaar verbonden zijn (de Autoriteit Persoonsgegevens schuwt immers de media niet), of dat dit wordt gestimuleerd door het aanscherpende toezicht vanuit (wederom) de AP, kan niet op basis van deze enquête worden geconcludeerd.





Bestuurders hebben deze vraag ook voorgelegd gekregen. Uit de beantwoording van bestuurders blijkt een zwaardere inschatting van de risico's dan bij de CISO's. Behalve op het onderwerp financiële schade is de riscoperceptie op alle onderwerpen bij bestuurders aanmerkelijk hoger. Daarbij springen de risico's van schade aan publieke opinie en vertrouwen van clienten eruit. Ook nemen bestuurders het risico van onherstelbare discontinuiteit aanzienlijk meer serieus dan de CISO's.

In het onderstaand schema zijn de verschillende risicopercepties met elkaar vergeleken.

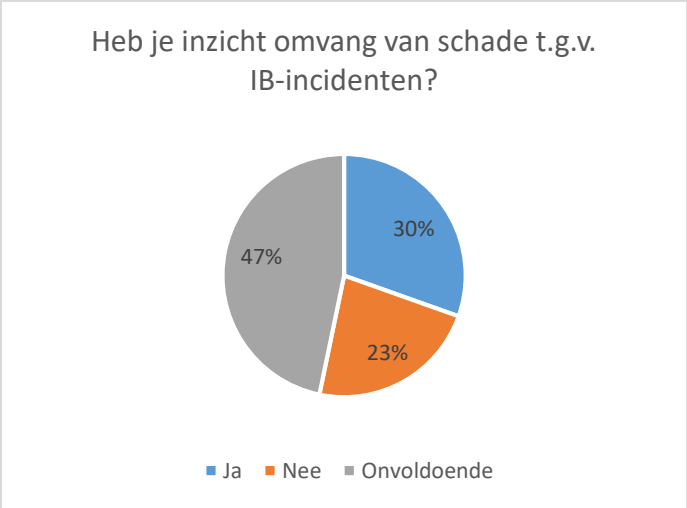


9.2 Zicht op de omvang van schade

Desgevraagd geven de responderende CISO's aan slechts in beperkte mate zicht te hebben op de omvang of het effect van IB-gerelateerde schade bij incidenten. Slechts 30% geeft aan daarop voldoende zicht te hebben. De resterende 70% geeft te kennen daarop onvoldoende (45%) of zelfs helemaal geen zicht (25%) te hebben.

Uit de beantwoording dringt zich het beeld op dat er weinig harde gegevens bekend zijn bij de CISO's uit risicoanalyses. Dit kan betekenen dat ze nog weinig worden uitgevoerd, ofwel dat ze weinig specifiek worden uitgevoerd.

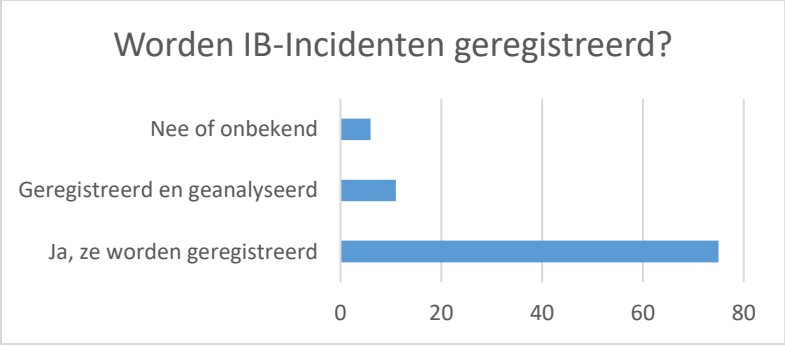
Voor goede afwegingen en prioriteitsbepaling van maatregelen en bijbehorende investeringen, is het van belang dat risicoanalyse met enige scherpte wordt uitgevoerd. Ook de toepassing van de BIO veronderstelt dit.



9.3 Registratie incidenten

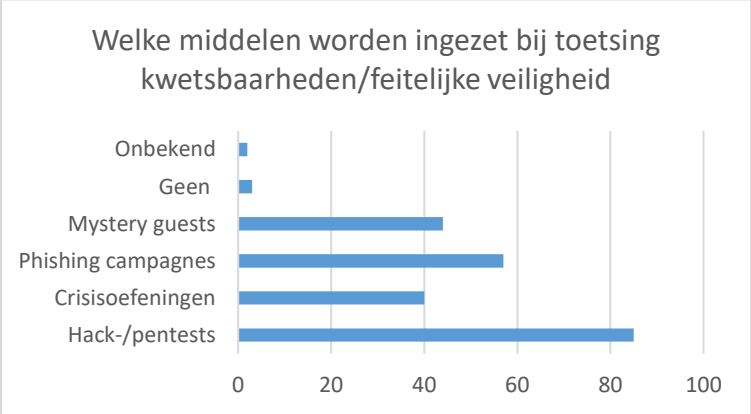
Bij veel respondenten (81%) worden IB-incidenten geregistreerd. Slechts in 12% van de gevallen worden ze ook geanalyseerd.

Wellicht heeft het kleine percentage 'geanalyseerd' te maken met het gegeven dat veel meldingen in het filter blijven hangen van de GRC-tooling en niet tot analyse leiden. Nader onderzoek zou nodig zijn om dit beeld te bevestigen.



9.4 Testen en oefenen

In het kader van het toetsen van feitelijke veiligheid is het van belang dat regelmatig getoetst wordt op de veiligheid van de organisatie en de IV-infrastructuur. Een aantal specifieke methoden zijn in de enquête uitgevraagd. Bij deze vraag konden meerdere toetsingsvormen worden aangegeven. De beantwoording levert het volgende beeld op.



Bij 92% van de organisaties worden *hack-/pentests* uitgevoerd. *Phishing* campagnes komt in 62% van de organisaties voor, *mystery guests* in 48% en crisisoefeningen in 43% van de organisaties.

Rond crisisoefeningen is gevraagd naar de regelmaat waarmee die worden gehouden. Slechts 30% van de organisaties houdt die met regelmaat: één maal per jaar of frequenter.

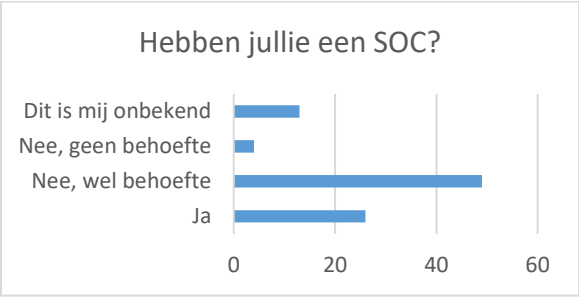
Bij deze vraag werden ook opmerkingen gemaakt. Daaruit blijkt dat in een aantal gevallen ook kwetsbaarheidsscans worden uitgevoerd. Naar schatting vindt dat in ca 10% van de organisaties plaats.

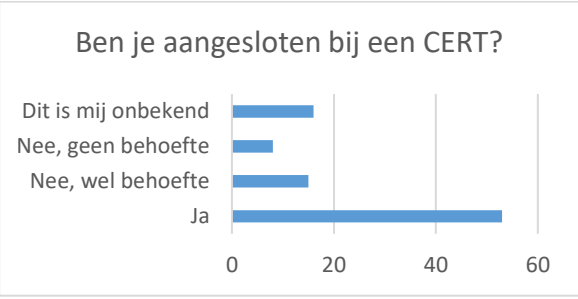
9.5 Borging van signalering en response

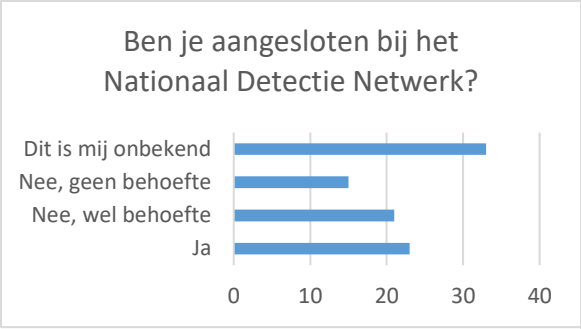
Voor het feitelijk veilig houden van de organisatie is het nodig dat signalering en response op incidenten structureel is geborgd. Dat kan op verschillende – soms elkaar versterkende - wijzen gestalte krijgen. In de enquête is de vraag gesteld naar het gebruik c.q. lidmaatschap van de volgende vormen:

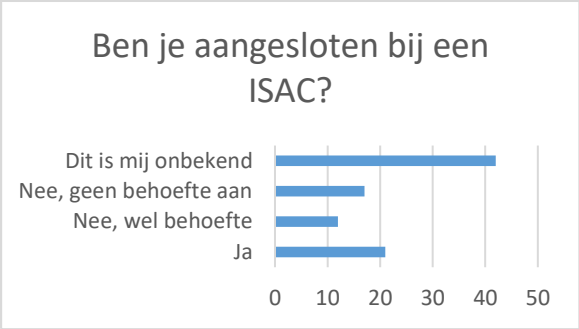
- heeft men een SOC (Security Operations Center) in de organisatie,
- is men aangesloten bij een CERT (Computer Emergency Response Team),
- is men aangesloten op het NDN (Nationaal Detectie Netwerk),
- is men aangesloten bij een ISAC (Information Sharing & Analysis Center).

De volgende diagrammen geven de beantwoording weer.









Bij het SOC
Slechts 28% van de organisaties maakt gebruik van een SOC. Dit is nog erg laag. Een groot deel wil het wel gaan doen (53%). Opvallend is dat er in deze verhoudingen geen wezenlijk onderscheid is tussen grotere en kleinere organisaties.

Uit de opmerkingen bij deze vraag blijkt dat de meest voorkomende vormen van SOC's zijn:

- eigen SOC,
- SOC van een partner of ICT-leverancier,
- SOC van een shared service center,
- aansluiting bij GGI-veilig.

Kleinere organisaties lijken i.h.a. aangewezen op uitbesteding.

Bij het CERT
Veel organisaties zijn lid van een CERT (58%). Hier wordt rol van de sectorale CERT's duidelijk zichtbaar. Veelvuldig worden genoemd: Watermanagement voor de Waterschappen, Informatie Beveiligingsdienst voor de Gemeenten, Z-CERT voor zorgsector en SURF-CERT voor hoger onderwijs.

Bij het NDN
De deelname aan het NDN is onder de respondenten nog niet groot (25%). 23% heeft er wel behoefte aan.

De reden voor de schaarse participatie is dat het NDN nu vooral gericht is op vitale sectoren en slechts een deel van de overheid. Het is aan te raden om het NDN toegankelijk te maken voor de gehele overheid. Dit kan leiden tot een verbeterde signalering van cyberdreigingen.

Bij het ISAC
De deelname aan een ISAC is onder de respondenten eveneens niet groot (23%). Nog eens 13% geeft aan er wel behoefte aan te hebben.

Ook ISAC's zijn er vooral in de vitale sectoren en het Rijk. Het zijn vertrouwde bijeenkomsten waarin op verschillende niveaus van vertrouwelijkheid wordt gecommuniceerd over incidenten en kwetsbaarheden. Waterschappen geven aan lid te zijn van ISAC 'Keren en Beheren'. Verder wordt het Zorg-ISAC genoemd.

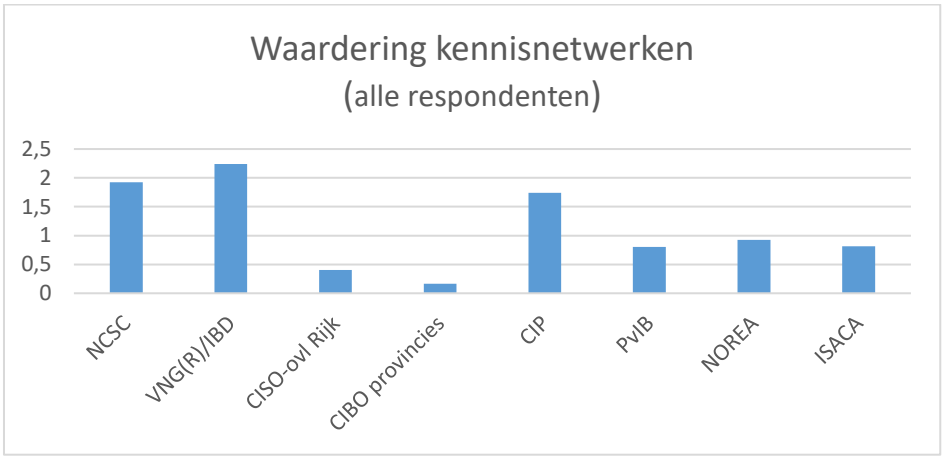
Het op neutrale wijze breder uitdragen van de uitwisselingen binnen de ISAC's, zou mogelijk een oplossing zijn voor degenen die niet kunnen deelnemen aan een ISAC. CIP zou hier t.g.t. een rol in kunnen spelen.

10 Kennisnetwerken

10.1 Benutting kennisnetwerken

We vroegen de respondenten naar de mate van ondersteuning die ze ervaren van kennisnetwerken buiten de eigen organisatie.

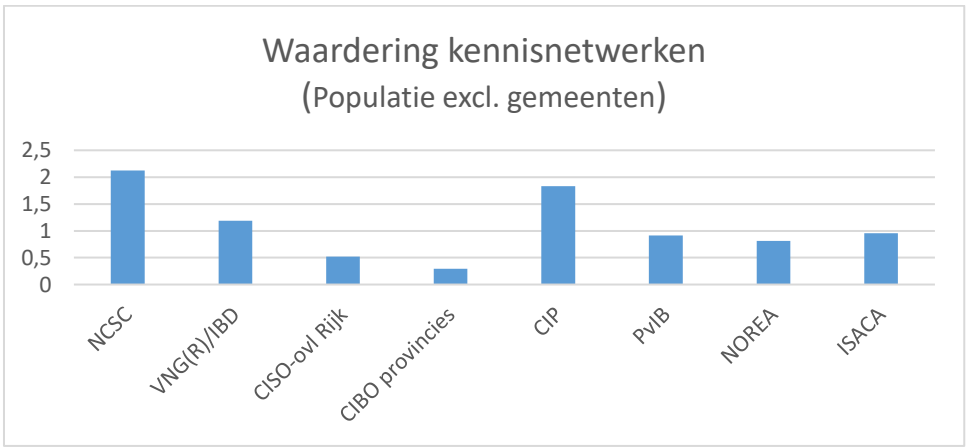
Voor een aantal kennisnetwerken/organisaties kon men aangeven of men weinig of veel ondersteuning ervaart. Als we de invullingen wegen (tegen 0 punten voor 'zeer weinig steun' tot 4 punten voor 'zeer veel steun'), dan blijkt het volgende beeld.



Kanttekeningen:

- De aard van de netwerken verschilt onderling. Sommige houden zich bezig met respons, andere alleen met preventie, of combinaties, soms gaat het alleen om bijeenkomsten. E.e.a. is dus niet zo maar vergelijkbaar.
- CIBO-provincies is alleen gericht op de provincies. Er zijn slechts 3 provincies onder de respondenten. Deze score heeft in deze vergelijking dus geen betekenis. Overigens waarderen de 3 responderende provincies het CIBO goed.
- Van het CISO-overleg is gericht op het Rijk. Ook deze populatie is te gering (11 respondenten) om uitspraken te doen n.a.v. de invullingen. Wel kan gesteld worden dat de 11 respondenten i.h.a. weinig steun ervaren van het Rijks-CISO-overleg.
- Van VNG(R)/IBD wordt de meeste steun gemeld, gevolgd door het NCSC, op de hielen gezeten door het CIP.

De helft van de respondenten komt uit gemeentekringen en daarom is dit beeld enigszins vertekend. Als we gemeentelijke respondenten uit de resultaten weglaten, wordt het plaatje iets anders. Het NCSC en het CIP blijken er dan uit te springen.



10.2 CISO-community

Bij 75% van de respondenten is steun voor het opzetten van de door CIP voorgestelde CISO-community. Een kleine helft daarvan geeft aan dat te willen beperken tot alleen overheidsmedewerkers. De resterende ca 25% geeft aan daar geen behoefte aan te hebben.

Hier volgen enkele van de belangrijkste kanttekeningen.

- Er zijn verschillende kringen die meestal niet heel erg werken.
- Liefst samen met IBD.
- Een aantal CISO's geven aan genoeg te hebben aan hun huidige netwerken.
- Zorg om versnippering.
- Geen Poolse landdagen.
- Tip om het regionaal te organiseren.

Bij enkele voor-gedefinieerde doelen kon men aangeven of men weinig of veel belang hecht aan dat doel. Als we de invullingen wegen (tegen 0 punten voor 'zeer weinig belang' tot 4 punten voor 'zeer veel belang'), dan blijkt het volgende beeld.

Hoewel de onderlinge verschillen niet erg groot zijn, kijkt men toch het meest naar onderling netwerken, met en van elkaar leren en kennis ontwikkelen.

Bijlage I. CISO Enquête - vragenlijst

Zie hieronder de vragen (vet) en de antwoordopties. Opgesplitst in 'voor CISO's' en 'voor bestuurders'.

Voor CISO's

1. **In welke sector o type organisatie ben je actief als CISO?**

   Departementaal
   Hoge Colleges van Staat
   Zorg
   Agentschap/uitvoerder
   Provinciaal
   Gemeentelijk
   Waterschappen
   ZBO
   Stichtingen en verenigingen
   Onderwijs/kennisinstituut
   Overige

2. **Aantal medewerkers in de (totale) organisatie?**
   1-100
   100-500
   500-1.000
   1.000-5.000
   5.000-10.000
   meer dan 10.000

3. **Aan wie rapporteer je?**
   Bestuurder (p)SG, DG, RvB-lid, e.d.
   Directeur
   CIO
   CFO
   Overig

4. **Oefen je in (een van) de organisatie(s) waarvoor je werkt naast de CISO-functie ook andere functies uit? [meerdere keuzes mogelijk]**
   De CISO-functie is mijn enige functie
   Mijn CISO-functie combineer ik met die van FG
   Mijn CISO-functie combineer ik met een ICT-functie
   Mijn CISO-functie combineer ik met andere functies
   Geef in de opmerking een schatting van het aantal uren dat je per week besteedt aan de rol van CISO

5. **Ben je in jouw organisatie ook verantwoordelijke voor Integrale Veiligheid?**
   Ja
   Neen

6. **Aansturing van medewerkers**
   Hoeveel medewerkers stuur je hiërarchisch aan?
   Hoeveel medewerkers stuur je functioneel aan?

7. **Over hoeveel budget (in duizenden €) kun je in 2019 beschikken?**
   Regulier
   Aanvullend voor projecten
   Decentraal

8. **Over hoeveel budget (in duizenden €) kun je naar verwachting in 2020 beschikken?**
   Regulier
   Aanvullend voor projecten
   Decentraal

9. **Wat is je leeftijd?**

10. **Wat is het hoogste niveau van je vooropleiding?**
    Middelbaar onderwijs
    MBO
    HBO
    WO
    Overig

11. **Over welke trainingen, opleidingen, certificaten beschik je zelf, relevant voor de CISO-functie?**

12. **Hoelang is je werkervaring in jaren?**
    In de functie van CISO?
    In de informatiebeveiliging?
    Sinds je begin met werken?

13. **Wordt het belang van informatiebeveiliging voldoende onderkend (1 = vrijwel niet; 5 = ja, volledig)**
    Bij bestuur/directie
    Bij management
    Bij medewerkers

14. **Waarmee houd jij je in je dagelijks werk als CISO mee bezig? [meerdere keuzes mogelijk]**
    Beleid
    Toezicht/audits
    Bewustzijn
    Advisering aan bestuur/directie
    Teammanagement
    Risicomanagement
    Crisis-afhandeling
    Organisatieverandering
    Inkoop/leveranciersmanagement
    Compliance
    Crisisafhandeling
    Overige

15. **Wat verwacht je van de rol van de bestuurder bij informatieveiligheid?**

16. **Wat zou in jouw beleving nog kunnen verbeteren in de samenwerking met de bestuurder?**

17. **Waarvan ondervind je in de uitvoering van je functie de grootste hinder? Geef per item op een schaal van 1-5 aan hoeveel hinder (1 zeer weinig – 5 zeer veel)**
    Gebrek aan steun bij bestuur/hoger management
    Gebrek aan steun middel/lager management
    Gebrek aan steun andere medewerkers
    Beperkte middelen
    Schaarse arbeidsmarkt
    Conflicterende belangen
    Beperkt mandaat/slagkracht in de praktijk
    Trage besluitvorming (interne of in de keten)
    Anders, nl

18. **Welke invloed heb je op de rapportage over informatiebeveiliging in het jaarverslag?**
    Ik schrijf de rapportage
    Ik lever input voor de rapportage
    Ik heb geen betrokkenheid bij de rapportage
    Over IB wordt niet gerapporteerd in het jaarverslag
    Ik weet niet of er gerapporteerd wordt over IB in het jaarverslag

19. **Wat is de stand van zaken m.b.t. het hanteren van de baseline?**
    Wij hanteren de BIO
    Wij hanteren de oude baseline (BIR, BIG, BIWA of IBI) en bereiden de overgang naar de BIO voor
    Wij hanteren de oude baseline (BIR, BIG, BIWA of IBI) en hebben nog geen plannen voor de BIO
    Wij hanteren de ISO 27001/2 en bereiden de overgang naar de BIO voor
    Wij hanteren de ISO 27001/2 en hebben nog geen plannen voor de BIO
    Wij hanteren een eigen kader en bereiden de overgang naar de BIO voor
    Wij hanteren een eigen kader en hebben nog geen plannen voor de BIO
    Onze situatie staat niet in dit lijstje

20. **Hebben jullie of streven jullie naar certificering op informatiebeveiliging.**
    Wij hebben de volgende certificering:
    Wij streven naar de volgende certificering:
    We hebben geen certificering en streven daar ook niet naar
    Dit is mij onbekend

21. **Gebruikt jouw organisatie GRC/ISMS tooling**
    Ja (vermeld de naam van de tool)
    Neen, maar dat willen we wel gaan doen
    Neen, wij hebben daaraan geen behoefte
    Neen, om de volgende reden:

22. **Hoe wordt informatiebeveiliging ingebracht bij IV-veranderingen?**
    Daar wordt geen of nauwelijks rekening mee gehouden
    De CISO heeft daarvoor beleid, maar heeft verder geen bijdrage bij IV-projecten
    De CISO licht het IB-beleid incidenteel toe bij IV-projecten
    De CISO licht het IB-beleid regelmatig toe bij IV-projecten
    De CISO heeft een actieve rol bij IV-projecten
    Overig:

23. **Welke informatiebeveiligingseisen stellen jullie – aanvullend op algemene inkoopvoorwaarden as ArbVodi, Arbit en GIBIT – aan leveranciers bij inkopen en aanbestedingen?**
    We stellen geen aanvullende eisen voor IB
    We eisen om te voldoen aan ISO 27001/2
    We eisen om te voldoen aan de BIO of een voorganger (BIR, DBIG, BIWI IBI)
    We eisen om te voldoen aan op de inkoop toegespitste kaders zoals SSD van de CIP
    Overig:

24. **Hoe schat jij voor jouw organisatie de grootste risico's in van incidenten op het gebied van informatieveiligheid? (1 = zeer klein; 5 = zeer groot)**
    Onherstelbare discontinuïteit van de dienstverlening
    Tijdelijke discontinuïteit van de dienstverlening
    Datalekken
    Schade aan vertrouwen bij cliënten van onze dienstverlening
    Schade aan ons imago/publieke opinie
    Verstoorde relatie met toezichthouder of departement
    Financiële schade (hertelkosten, proceskosten, boetes, e.d.)

25. Worden de ICT-voorzieningen en/of de organisatie periodiek getest op weerbaarheid en kwetsbaarheden?
Ja, meerdere keren per jaar
Ja, een keer per jaar
Ja, incidenteel
Neen, te ingewikkeld, tijdrovend of te duur
Neen, dat vinden wij niet nodig
Dat is mij onbekend

26. Welke middelen worden hierbij ingezet?
Hacktests/pentests
Crisisoefeningen
Phishing campagnes
Mystery guests
Dit is mij onbekend
Overig

27. Hoe vaak wordt crisisoefening gehouden?
Meerdere keren per jaar
Een keer per jaar
Incidenteel
Nooit
Dat is mij onbekend

28. Worden informatiebeveiligingsincidenten geregistreerd?

Neen
Ja, maar niet als zodanig geoormerkt
Ja, ze worden als beveiligingsincident geregistreerd
Ja, ze worden als beveiligingsincident geregistreerd en geanalyseerd
Ja, ze worden als beveiligingsincident geregistreerd, geanalyseerd en gerapporteerd
Dit is mij onbekend

29. Van welke van de volgende soorten incidenten ondervindt jouw organisatie de meeste schade (1 = heel weinig; 5 = heel veel)
Hacking/ongeoorloofde toegang
Virussen
DD0S-aanvallen
Phishing
Menselijke fouten
Fouten of kwetsbaarheden van leveranciers

30. Heb je inzicht in de omvang van de schade hierdoor?
Ja (hoeveel?)
Onvoldoende
Neen

31. Hebben jullie een SOC, dan wel maken jullie gebruik van een gezamenlijk SOC?
Ja (welke?)
Neen, maar ik heb er wel behoefte aan (om welke reden?)
Neen, ik heb er geen behoefte aan (om welke reden?)
Dit is mij onbekend

32. Ben je aangesloten bij een CERT?
Ja (welke?)
Neen, maar ik heb er wel behoefte aan (om welke reden?)
Neen, ik heb er geen behoefte aan (om welke reden?)
Dit is mij onbekend

33. **Ben je aangesloten bij het Nationaal Detectie Netwerk (NDN)?**
    Ja
    Nee, maar ik heb er wel behoefte aan (om welke reden?)
    Neen, ik heb er geen behoefte aan (om welke reden?)
    Dit is mij onbekend

34. **Ben je aangesloten bij een ISAC?**
    Ja (welke?)
    Neen, maar ik heb er wel behoefte aan (om welke reden?)
    Neen, ik heb er geen behoefte aan (om welke reden?)
    Dit is mij onbekend

35. **Van welke kenniskringen buiten de organisatie ervaar je steun op het gebied van informatiebeveiliging? (1 = zeer weinig steun, 5 = zeer veel)**
    NCSC
    VNG(-R)/IBD
    CISO Overleg Rijk
    CIBO Provincies
    CIP
    PvIB
    Norea
    ISACA

36. **Bij welke onderwerpen ben je graag betrokken in CIP-verband?**

37. **Zijn er onderwerpen waarvan je vind dat CIP die zou moeten oppakken naast het huidige aanbod?**

38. **Wat je de belangrijkste doelen voor een CISO-community (1 = zeer belangrijk; 5 = zeer belangrijk)?**
    Belangenbehartiging/spreekbuis
    Kennisontwikkeling en kennisdeling
    Kwaliteitsborging CISO functie-uitvoering
    Netwerken met vakgenoten
    Intervisie

39. **Ik heb nog de volgende suggesties voor de CIS-community**

Voor bestuurders/algemeen secretaris/directeur

1. **Tot welke sector of type organisatie behoort uw organisatie bestuurder?**
    Departementaal
    Hoge Colleges van Staat
    Zorg
    Agentschap/uitvoerder
    Provinciaal
    Gemeentelijk
    Waterschappen
    ZBO
    Stichtingen en verenigingen
    Onderwijs/kennisinstituut
    Overige

2. **Aantal medewerkers in de totale organisatie?**

   1-100
   100-500
   500-1.000
   1.000-5.000
   5.000-10.000
   meer dan 10.000

3. **Wat is uw functie?**

4. **Hoe ziet u uw eigen rol inzake informatieveiligheid?**

5. **Op welke onderdelen verwacht u activiteit van de CISO?**

   Beleid
   Toezicht/audits
   Bewustzijn
   Advisering aan bestuur/directie
   Teammanagement
   Risicomanagement
   Crisis-afhandeling
   Organisatieverandering
   Inkoop/leveranciersmanagement
   Compliance
   Crisisafhandeling
   Overige

6. **Wat zou in uw beleving nog kunnen verbeteren in de samenwerking met de CISO?**

7. **Welke stellingen gelden voor uw organisatie? (ja/neen)**
   Informatieveiligheid is gewoon onderdeel van de bedrijfsvoering
   Informatieveiligheid wordt bestuurd als onderdeel van onze planning & control-cyclus
   Verbetering van de Informatieveiligheid is een speerpunt voor ons
   Informatieveiligheid is bedrijf-kritisch voor ons
   Informatieveiligheid behoeft bij ons geen bijzondere aandacht

8. **Wat zijn voor uw organisatie de grootste risico's van incidenten op het gebied van informatieveiligheid? (1 = zeer klein; 5 = zeer groot)**
   Onherstelbare discontinuïteit van de dienstverlening
   Tijdelijke discontinuïteit van de dienstverlening
   Datalekken
   Schade aan vertrouwen bij cliënten van onze dienstverlening
   Schade aan ons imago/publieke opinie
   Verstoorde relatie met toezichthouder of departement
   Financiële schade (herstelkosten, proceskosten, boetes, e.d.)

9. **Heeft u tips die CIP als kennisdelingsplatform zou kunnen meenemen in het activiteitenprogramma van 2020?**

Bijlage II. Gevolgde specifieke opleidingen

Welke specifieke zijn gevolgd die van belang zijn voor de CISO-functie?
- Information Security Practitioner - Data Protection Practitioner - IT-Security Practitioner
30 trainingen. Certificeringen: CISSP, CISA, CCSP CIP/e opleiding en BCM opleiding
AMBI-modules, RE (lid NOREA)
Bedrijfskundige Informatica (HBO); audittrainingen; 2 daagse CISO training van BMC regionale bijeenkomsten met collega CISO's en landelijke bijeenkomsten van IBD en ENSIA
Bezig met CISSP
CEH, ISO27002, Advanced Infrastructure Hacking
Certified Security Manager, ISO/IEC27001
CIPP/e CISSP CISM CCSP
CISA, CISM, CIPP/E, CIPM, FIG
CISA CISM CRISC CGEIT CISSP CCSP CIPP/E CIPM ISO27001 Lead Implementer ISO 27001 Lead Auditor SABSA Foundation SABSA Practitioner PRINCE2 Practitioner
CISA CSIM
CISA, CDPO
CISA, CIS, CRISC
CISM
CISM training, examen gepland
CISM CIPM CIPP/E CIPT CISSP MCSE: Security Prince2 ITIL
CISM,
CISM, CIPP/E
CISM, CISA
CISM, CISSP en verscheidene meer gespecialiseerde waaronder Threat Intelligence en Cryptografie
CISM, CRM (27005 en 31000), CIPT, toegepaste cryptografie
CISM, CRM ISO27005, CIPP/E, CIPM, CMP
CISM, Lead auditor ISO27001, CIPP/E.
CISM, SIOO verandermanagement
CISO (incl. certificering
CISO (Segment)
CISO certificaat training Diverse ICT-gerelateerde trainingen Diverse trainingen op gebied van communicatie
CISO masterclass
CISO Masterclass CISM Training
CISO opleiding
CISO opleiding en Security awareness opleiding, hacken
CISO Training (SEP)
CISO voor gemeenten, Risicomanagement en binnenkort CISA
CISO-opleiding Hogeschool Management Documentaire Informatievoorziening (HMDI)
CISO-opleiding, HBO Information Security Management,
CISSP

CISSP CISM
CISSP opleiding, CISM opleiding, ICS RT/BT, security opleidingen intern
CISSP, CCISO, CEH, CGEIT, risk management
CISSP, CHE, CISA, etc. een hele reeks
CISSP, CISA, CIPP/E
CISSP, CISA, CISM, C|CISO, CEH, Togaf, Cobit, CRISC, ITIL
CISSP, CISM, CCFP
CISSP, CISM, CIPP/E
CISSP, CISO
CISSP, geen examen gedaan wel zonder problemen gevolgd
CISSP, SICA
CISSP,CIMS,CISA
dagjes cursus
Diverse Masterclasses gevold via M&I Partners Heb 30 jaar in de ICT techniek gewerkt als sr. medewerker ICT gecombineerd met de functie Beleidsadviseur ICT
Druk bezig met CISSP
geen
Geen, kwam telkens er niet van dat er een opleiding gevolgd werd. Wil mij wel heel graag laten certificeren.
Geen.
HBO Bedrijfskundige Informatica CISO-opleiding CSX cyber (via ISACA)
HBO plus IT auditing, CISA ISACA, CRISC ISACA
HBO-BI en post-HBO Privacy Management
HTS-computertechniek en vele techniekcursussen erna. IT-audit opleiding Tias Nimbas
ICT-opleiding, V-ICT-OR opleiding informatieveiligheid, en diverse korte opleidingen en seminaries i.v.m. informatieveiligheid en privacy.
Informatiebeveiliging voor gemeenten (Security Academy), CISO opleiding (Segment), CISO Masterclass, CCSP (geen examen gedaan)
Informatiebeveiligingsopleiding
Information Security Foundation/Practitioner (ISF/ISP) Privacy & Data Protection Foundation Certified Information Systems Security Professional (CISSP)
Ir informatica
ISMP
ISO lead auditor
ISO1: ir Informatica + RE + CIPP/E ISO2: ing. Analytische Chemie + MCSE + CISA + COS
ISO27001 lead auditor; CISO-C
ISO27001 lead implementer ISO27001 lead auditor
IT-auditor TIAS Nimbas
MBA, Bedrijfskunde, Basisdiploma AMBI, AS400 opleiding
MBA, informatiemanagement en privacy training
MIM
n.v.t.
NEN ISO27001-training
Nog geen specialistisch opleiding. Start in september / oktober met de opleiding van Segment.
Nyenrode Business Universiteit
Opleiding CISO via Segment (nu SEP)
Opleiding FG, Training en masterclass CISO,
Opleiding Information Security Management
Post Doctoraal Information Security Management Post Doctoraal Master of Information Management Post Doctoraal Bestuurlijke Informatie Kunde Post HBO Bedrijfskundige Administratieve Organisatie

HBO HRM Gecertificeerd CISO en DPO, Authorized Trainer.
RE en CISA
RE opleiding
Register EDP Auditor
S-CISO CISSP
S-ISP van de Security Academy
S-ISP, CISM, CCSP
Trainee-ship Informatiemanagement Verder alleen bijeenkomsten/presentaties gevolgd
Training ITIL
training on the job door ervaren CISO
Trainingen ISO, Risk, privacy etc.
twee 5-daagse CISO trainingen via twee van de adviesbureaus die actief zijn in deze business
Veel technische ICT trainingen.
Verschillende certificaten.
WO Managementwetenschappen (verandermanagement)
Zelfstudie, CIP-dagen en andere conferenties, Informatieveiligheid en privacy in de praktijk

Bijlage III. Verwachtingen van de CISO over de rol van bestuurder

Wat verwacht je van de rol van bestuurder bij Informatieveiligheid?
Sponsor
1e lijn is verantwoordelijk voor informatiebeveiliging. CISO monitort of de lijn het beleid implementeert en naleeft.
Actief handelen en goede voorbeeld
Actief het beleid accepteren en uitdragen.
actief vragen om informatie. risicomanagement op dat niveau uitvoeren.
Actieve steun
Active uitdraging in de organisatie
Ambassadeur en boegbeeld voor dit taakveld
Ambities en doelen stellen, helder prioriteren van informatieveiligheid t.o.v. andere bestuurs-thema's. Onderkennen en uitdragen belang/noodzaak van informatieveiligheid, specifiek naar (lijn)management en medewerkers Positioneren CISO en FG
Begrip, inbreng en bijdrage aan informatieveiligheid gerelateerde zaken. Waaronder (enigszins) kennen van vakgebied, kunnen aangeven wat de kroonjuwelen zijn gezien vanuit de bestuurskamer, en bijdragen aan actief mobiliseren van directie en managementteams op IB-gebied.
Begrip, steun, commitment
Beslissingen nemen aan de hand van advies dat ik geef, 'vechten' voor het belang van informatieveiligheid bij raad, het op de agenda houden, budget beschikbaar stellen.
Betrokkenheid
Betrokkenheid en bewustzijn (is eindverantwoordelijk)
Betrokkenheid en ondersteuning waar nodig.
Betrokkenheid, steun (zowel financieel als bij creëren draagvlak) Ook het nemen van verantwoordelijkheid en eigenaarschap.
Bevorderen bewustzijn van beveiliging: uitdragen nut en noodzaak. Betrokkenheid tonen, voorbeeldfunctie.
Bijdrage kunnen leveren aan en het uitdragen van de vertaling van de visie en missie (collegeprogramma) in die voor informatieveiligheid/privacy en de vertaling in risico's in geld en imago.
Boegbeeld, belang aangeven
Commitment
Commitment – zeggen dat je het belangrijk vind en het daarbij behorende gedrag vertonen
Commitment afgeven, richting geven
Commitment en bevestiging van sturing op verbetering. Zorgen voor rust in geval van incidenten.
commitment en voorbeeld gedrag
Commitment van de bestuurder, mens & middelen beschikbaar stellen, voorbeeld geven aan de organisatie en het onderwerp bespreekbaar maken en op de agenda zetten.
Dat de bestuurder het belang van informatieveiligheid voor de organisatie begrijpt en dat uitstraalt naar de rest van de organisatie. Dat de bestuurder de nodige budgetten vrij maakt om activiteiten te ondernemen om informatieveiligheid te verbeteren.
Dat de bestuurder ook het belang van informatieveiligheid onderkent en zo nodig ook zich hard maakt voor het beschikbaar stellen van het benodigde budget.
Dat deze de CISO optimaal faciliteert
Dat het belang van informatieveiligheid wordt ingezien en uitgedragen er de noodzakelijke resources voor vrij worden gemaakt.
Dat hij/zij het belang ervan inziet, dit uitdraagt en er ook naar handelt, er voldoende middelen (personeel en geld) voor vrijmaakt.
Dat hij/zij sturing geeft aan de prioriteiten en support geeft aan de voorstellen
Dat hij/zij zicht bewust is van de risico's en zich daarover laat informeren, dan wel informeert hoe het ermee staat.

Dat informatieveiligheid ook echt serieus genomen wordt. Meestal wanneer het er op aan komt dat ze een keer moeten kiezen voor informatieveiligheid in plaats van de kosten die het heeft of verandering in werkwijzen dan wordt toch in het voordeel van de andere factoren gekozen en niet voor informatieveiligheid.
Dat zij hun verantwoordelijkheid nemen. In gemeenteland ontbreekt veelal de tactische laag. Komst dat dat gewerkt wordt met teamleiders die zich niet met de inhoud mogen bemoeien en de zelfsturende teams die niet goed weten hoe zij dit in moeten vullen.
De bestuurder is integraal eindverantwoordelijk, samen met de directeur/secretaris die ambtelijk eindverantwoordelijk is. Samen met de CISO vormen ze een driehoek, waarin de verantwoordelijkheid voor de PDCA cyclus t.b.v. informatieveiligheid wordt gespeeld. De CISO rapporteert rechtstreeks aan hen.
De bestuurder is verantwoordelijk en dient het (hogere) management zodanig aan te sturen dat zij zich ook verantwoordelijk voelt
De bestuurder moet het goede voorbeeld geven.
Draagvlak en bewust nemen van besluiten (o.b.v. risico management)
Dragen van verantwoordelijkheid en sturing op het onderwerp.
Een adverterende rol. M.a.w. het belang dat het bestuur hecht aan IV uitdragen
Een duidelijke visie, betrokkenheid.
Een luisterend oor en initiërend richten gemeenteraad
Een mandaat
Een voorbeeldfunctie op het dossier Informatieveiligheid Voorwaardenscheppend Medewerkers bewust maken van het belang en beveiligen van informatie
Eigenaarschap
eigenaarschap en verantwoordelijkheid
Eigenaarschap pakken ontbreekt volkomen. Bestuurders kijken weg, hebben geen interesse en nemen de risico's niet serieus.
Eigenaarschap van het vakgebied, en commitment
Eindverantwoordelijkheid bij nemen van beslissingen.
Geïnformeerd willen zijn vanuit oogpunt organisatiebelang; keuzes maken/prioriteren t.a.v. geld en menskracht o.b.v. risico.
Geven van committent aan security doelstellingen, ter beschikking stellen middelen, opstellen bedrijfsdoelen, bepalen 'risk appetite'.
Goede voorbeeldrol, Informatiebeveiliging risico management borgen en betrokkenheid bij het onderwerp Informatieveiligheid actief uitdragen
Goedkeuring voor doorvoeren van security verbeter initiatieven Ondersteunen voor security awareness campagnes
Grote afstand omdat ik werk bij ZBO, bij de gemeente is dit anders
het belang van informatie en beveiliging van informatie zien en dat uitdragen.
Het geven van commitment en het leveren van de juiste middelen aan de uitvoeringsverantwoordelijken voor het implementeren van risico-reducerende maatregelen.
Het respectvol afwegen van belangen, het goed geïnformeerd zijn, en een realistische visie.
Het uitdragen van hoe belangrijk het is
Ik verwacht een actieve aanjagende rol van de bestuurder waarmee deze de urgentie van het onderwerp afstraalt op de medewerkers. Met als doel dat deze zelf ook nadenken over beveiligingsvraagstukken in hun dagelijks werk.
Inhoudelijk hoeft hij/zij dit niet helemaal te snappen, maar hij/zij moet wel begrijpen dat het belangrijk is, en dat ook uitdragen. Goed voorbeeld gedrag is key.
Invullen van randvoorwaarden Voorbeeldgedrag
Kaderstellend en controlerend naar de interne ambtelijke organisatie en als portefeuille houder vaandeldrager. Naar de collega bestuurders als enthousiasmerend
mandaat.
Meedenken, steun bij benodigde besluitvorming
Meenemen in de beleidsvelden en overleggen met afdelingsmanagement. Zichtbaarheid op het vakgebied.
Meer betrokkenheid en een duidelijke visie op het gebied van informatiebeveiliging
Meer betrokkenheid en verantwoordelijkheidsgevoel
Meer bewustzijn van informatieveiligheid en verantwoordelijkheid nemen voor risico's
Motivator met voorbeeld gedrag. Enabler door vaste agendering op directie / management niveau.

Nut en noodzaak van risicobeheersing en compliance erkennen, daarvoor kader en richting af te geven, resources beschikbaar te stellen en daar waar nodig bij te (laten) sturen.
Ondersteunend en verantwoordelijk. De verantwoordelijkheid voor informatieveiligheid ligt bij de lijn en niet bij de adviseur. Uitvoering van geadviseerde maatregelen en controls is een verantwoordelijkheid van de lijn
Ondersteuning, actief uitdragen, belangstelling over stand van zaken
Onvoorwaardelijke ondersteuning en onderschrijving van het belang
Optreden als voorbeeldfunctie, als sponsor.
Organisatiekaders afgeven, Controleren, rapporteren
Overleg over visie en strategie. Steun bij problemen.
Pro-actiever het is nu vaak een kwestie van brengen het moet meer een wisselwerking worden, er worden nooit vragen gesteld alleen als er iets mis gaat.
Randvoorwaarden voor een goede IB
Risicomanagement op gebied van informatiebeveiliging integreren met de bestaande besluitvormingsprocessen.
Staan voor de zaak. Dat betekent in doen en handelen zelf het goede voorbeeld geven, maar ook als boegbeeld en steun fungeren als er een extra zet nodig is.
Steun
Steun aan de CISO om de organisatie mee te trekken naar voren
Sturen op prioriteiten
Sturing, besluitpunt o.b.v. advies
Sturing, prioritering, resources
Supporter, medewerkers aangeven dat het belangrijk is en verwacht wordt.
Supporter, moet uitdragen dat dit een kerncompetentie moet worden. Het moet in ons dna gaan zitten.
Uitdragen beleid Informeren raad en veilig stellen van budget
Uitdragen van beleid en uitgangspunten.
Visie, draagvlak en budget
Voldoende kennis/bewustzijn op bestuurlijk niveau Gesprekspartner Bewust omgaan met risico's Verantwoordelijkheid nemen
Volledige ondersteuning en medewerking.
Voorbeeld gedrag is essentieel.
Voorbeeld gedrag, voldoende faciliteren
Voorbeeld rol
Voorbeeldfunctie en actief uitdragen van belang van informatieveiligheid. Beleid vaststellen en periodiek communiceren naar organisatie
Voorbeeldfunctie en interesse
voorbeeldfunctie vervullen, daadwerkelijk prioriteit geven aan informatiebeveiliging
Voorbeeldfunctie, ambassadeur, facilitator
Voorbeeldfunctie, ondersteunen van het belang van informatieveiligheid, lange termijn visie
Voorbeeldfunctie, uitdragen bewustzijn informatieveiligheid.
Voorbeeldgedrag, Security verantwoordelijkheden ook neerleggen bij lijnmanagement, sponseren van relevante projecten.
Voorbeeldgedrag. Promotor.
Voorbeeldrol en sturend. Ook: verantwoording nemend en afleggend aan de Raad.
Wat is het verschil tussen informatieveiligheid en informatiebeveiliging? Die eerste ken ik niet. Dus ik neem aan dat IB bedoeld wordt. Heeft een voorbeeld rol. Moet commitment tonen in word EN gedrag. Stelt prioriteiten bij escalaties en is overall eigenaar van de risico's en risk-appetite (risico acceptatie bereidheid) Keurt het beleid goed
Weet welke risico's er zijn en of hij deze wel of niet wil accepteren. Voorbeeldgedrag. Wil rechtstreeks op de hoogte willen gehouden
Wijsheid en inzicht
Zie de "De 10 bestuurlijke principes voor informatiebeveiliging"

Bijlage IV. Hoe ziet de bestuurder zijn eigen rol

Aanjager
Aansturing van CISO, verantwoordelijk voor digitale weerbaarheid en privacybescherming in organisatie (beleidsmatig en initiërend, control).
CISO rol, verantwoordelijk voor PDCA cyclus Informatiebeveiliging o.b.v. ISO27001 Organisatie hier actief in meenemen; beheer ISMS, rapportages, advisering Directie
Eindverantwoordelijk
eindverantwoordelijk en boegbeeld
sturend, zowel ten aanzien van de harde als de zachte kant.
Uitdragen belang IB&P en van het belang te voldoen aan wettelijke kaders. Balans aanbrengen tussen IB&P en andere belangrijke onderwerpen, zoals dienstverlening.
Verantwoordelijk voor geode inrichting van informatiebeleid. Escalatie beslisser bij iv versus andere uitvoeringsdilemma
Bestuurlijk Portefeuillehouder
Eigenaar Preventie Privacy by design Gedragsbeïnvloeding/ bewustwording Aanspreken/ handhaving
In ons IB plan heb ook ik elke jaar enkele acties uit te voeren. Voorbeeldfunctie als directeur is uitermate belangrijk. I.k.v. hygiëne vraag ik regelmatig aandacht voor informatieveiligheid waarmee ik het team van security officer en FG help de waarde hiervan blijvend te laten doordringen in de organisatie. Ten tijde van incidenten ben ik op de hoogte van informerend tot escalerend (cf escalatie ladder etc)
Kaderstellend Voorbeeldrol Bewustzijn in de organisatie vergroten
Portefeuillehouder dus bestuurlijk verantwoordelijk voor informatieveiligheid.
Verantwoordelijk
Verantwoordelijk voor de opzet & borging van informatieveiligheid.
Verbindend tussen organisatie, techniek en bedrijfsvoering (audits)
Voorbeeldfunctie Sturen volgens onze kernwaarden
CISO, BVC, Privacy Officer en Control rapporteren rechtstreeks aan mij. Daarnaast is er een portefeuillehouder Beveiliging vanuit de lijn benoemd.
De CISO is verantwoordelijk voor de kwaliteit van / de bekendheid met / de controle op de uitvoering van het informatiebeveiligingsbeleid. De uitvoering van het informatiebeveiligingsbeleid is een verantwoordelijkheid van het lijnmanagement
Eindverantwoordelijk
Faciliteren dat sprake is van awareness rondom dit thema in de organisatie, zorg dragen dat informatieveiligheid periodiek wordt ge-audit en dat maatregelen (zowel technisch als organisatorisch) structureel adequaat zijn genomen.
Aspectverantwoordelijke organisatie-breed
Faciliteren en controleren
Het is mijn verantwoordelijkheid zeker te stellen dat de processen en procedures zorgen voor passende informatieveiligheid, en ik zie het als mijn verantwoordelijkheid een omgeving te creëren dat medewerkers het signaleren als er sprake van gebreken zouden zijn (informatieveiligheid, maar ook anderszins) en waar mogelijk zelf maatregelen nemen.
Uitdragen op bestuursniveau Bewaken kaders Faciliteren in uitvoering
Verantwoordelijk
Ik ben als algemeen directeur eindverantwoordelijk voor het reilen en zeilen van de organisatie, daar hoort bij hoe wij omgaan met informatie-veiligheid en hoe dat is belegd.
Opdrachtgever, verantwoordelijk lijnmanager
CIO

Verantwoordelijk voor een deugdelijke en juiste informatievoorziening, inclusief bedrijfssystemen (SCADA)
Bestuurder eindverantwoordelijk, controller gemandateerd verantwoordelijk
eindverantwoordelijk voor ordentelijke informatiebeveiliging binnen organisatie
Heeft Prioriteit wegens belang. Wegens beperkte omvang hebben we geen CISO. Mede daardoor ben ik directer betrokken. Flankerend samenwerking binnen KleinLef en regelmatig overleg JenV op hoofdlijnen. Weinig concrete hulp van JenV.
Verantwoordelijk voor het leveren van veilige Informatie systemen.
1. Verantwoordelijk voor informatieveiligheid binnen directie. 2. Verantwoordelijk directeur voor alle onderzoeken die de AR doet op terrein van informatieveiligheid en Cybersecurity

Bijlage V. Wat kan volgens de CISO verbeteren in de relatie met de bestuurder

Wat zou in jouw beleving kunnen verbeteren in de samenwerking met bestuur?
Aangezien risicomanagement op het gebied van informatieveiligheid nog nieuw is in onze organisatie, moet die spel nog "op de wagen komen". Ook de samenwerking met de bestuurder moet nog groeien op dit punt. Is nu nog wat ad hoc.
Algehele bewustwording bij bestuurders, kritische vragen stellen
Begrip voor de veelal aanwezige tegenstelling tussen gebruikersvriendelijkheid versus beveiliging. Ofwel meer bewustwording van de risico's die er zijn maar veelal voor gebruikers (en bestuurders) niet direct zichtbaar zijn. Bijv. gebruik van internettool om "even iets thuis in pdf om te zetten" waarmee een intern document ineens op straat/internet komt te liggen.
Belang
Benadrukken van de waarde van informatie
Bestuurder kan op hoofdlijnen meer meedenken bij bepalen van de marsroute voor IB.
Bestuurder moet digitaler worden om mee te beginnen, zicht krijgen op integrale risico's en periodiek table-top oefeningen meedoen.
Bestuurder zou hier meer rechtstreekse betrokkenheid bij moeten hebben, o.a. bij de bepaling van de risico's en de te nemen maatregelen
Betrokkenheid
Bewust nemen van besluiten.
Bewustwording
Bewustwording over de dreigingen en risico's waar we als organisatie mee te maken hebben.
Bewustwording over de dreigingen en risico's waar we mee te maken hebben en waar wij als informatiebeveiligers ons tegen beschermen.
bredere visie op informatie en informatiebeveiliging
Budgetten en I-Veiligheid beter geborgd in de calamiteitenorganisatie
Burgemeester is bij ons portefeuillehouder. Hij vindt het onderwerp, tezamen met privacy, belangrijk en dankzij hem heb ik al meerdere zaken voor elkaar gekregen die bij lager niveau lastiger zouden gaan.
Communicatie momenten en relatie, op dit moment zeer beperkt gesprekken met de bestuurder
Dat de taken en verantwoordelijkheden worden belegd en dat wordt gestuurd. Zet de governance goed neer.
Dat hij actief handelt en ook het goede voorbeeld geeft
Dat we beter op elkaar ingespeeld raken
Dat we dezelfde taal spreken en dat de informatieveiligheidsrisico's in het risico-denken van de bestuurder past.
De bestuurder hoeft informatiebeveiliging niet alleen over te laten aan de expertise van de CISO, maar mag zelf actief in gesprek gaan.
De bestuurder zou het belang van IB veel meer moeten onderkennen en dit moeten ondersteunen en uitstralen naar de organisatie. Dit gebeurt nu niet waardoor er weinig gebeurt op dit gebied in de IB (lage prioriteit).
De lat nog wat hoger leggen rond proactieve weerbaarheid...
Denk dat de bestuurder het onderwerp prima kan mandateren naar management.
Directer contact
Doordat in een gemeentelijke setting elke 4 jaar het bestuur (College van B&W) wisselt is het weer opnieuw nodig om informatiebeveiliging ook bestuurlijk op de agenda te zetten. Dan zou we nog beter kunnen doen, ook in samenwerking met VNG / IBD.
Duidelijker governance structuur
Duidelijker maken welke beslissingen en sturing er naar de organisatie moet.
Een gezamenlijke visie ontwikkeling en een heldere beleid
Een keer overleg zou al mooi zijn
Effectiviteit, slagkracht
Er moeten meer resources beschikbaar komen om te kunnen omgaan met de steeds complexere regelgeving (zowel interne als externe regelgeving). Wanneer dit niet mogelijk is zal de bestuurder moeten accepteren dat security niet optimaal gewaarborgd is.
Expliciete sturing binnen organisatie op informatieveiligheid op basis van periodieke rapportages
Frequenter bijpraten

Gaat goed
geen idee los van bovenstaande
Gerichte ondersteuning vanuit de overheid.
Het aanspreken van het management op de 1e lijnverantwoordelijkheid.
Het belang ervan vertalen in uitvoering, door meer capaciteit en budget ter beschikking te stellen.
Het besef dat informatiebeveiliging integraal onderdeel is van de bedrijfsvoering
Het bewustzijn van bestuurders vergroten. Dit is nog een verbeterpunt (ook landelijk). Het is nog te weinig tastbaar.
Het gaat eigenlijk best goed voor wat betreft de portefeuillehouder. Interesse en betrokkenheid van andere bestuurders kan beter.
Het gesprek voeren over de kwaliteitsverbetering met een passende integrale aanpak in de organisatie inzake gegevensveiligheid. Mogelijk aanpassen / inpassen in de structuren die er al zijn zoals b.v. sociale veiligheid, fysieke veiligheid.
Het vaststellen van de behoefte aan management informatie
Ik ben best tevreden met het bestuur. We zouden meer risico-gedreven kunnen werken.
Ik merk dat bestuurders nu alleen reageren als er daadwerkelijk incidenten zijn, die reputatieschade of datalekken met zich meebrengen. Daarvoor is de betrokkenheid minimaal.
Ik vind de bestuurder te afwachtend. Ik moet zelf met voorstellen komen. Andersom wordt er nauwelijks gevraagd om actie of naar voortgang. Ook vervult de bestuurder onvoldoende de hierboven beschreven rol.
Informatieveiligheid hoger op agenda.
Intensiever contact (kan ik zelf wat aan doen).
Interesse bij bestuurder voor IV
Intrinsieke motivatie voor het onderwerp
Is net nieuwe burgemeester, moet er nog wel wat ingroeien
Kennis van security bij bestuurders
Kennis.
Lasting
Mandaat
Meer (informeel) contact buiten de reguliere contactmomenten om.
Meer aandacht voor het onderwerp en de noodzaak. Mijn ambitieniveau ligt hoger dan bij de bestuurder; wat ook wel weer logisch is. Informatieveiligheid is mijn speerpunt, voor de bestuurder is het 1 van de vele portefeuille onderwerpen.
Meer aandacht voor het onderwerp en erkenning voor het werk. Dat zij ook echt achter het advies staan en het ook uitdragen.
Meer begrip (over en weer) kan altijd. Dat kost echter meer tijd en die wordt niet altijd gegund.
Meer directe ondersteuning en meer vertrouwen; een voorgestelde maatregel die echt noodzakelijk is om risico's te mitigeren moet niet van tafel geschoven kunnen zonder daar onderbouwd en aantoonbaar verantwoordelijkheid voor te nemen
Meer frequent / gepland overleg met CEO Met COO in place
Meer in gesprek gaan over het voorgaande.
Meer kennis van informatiebeveiliging en meer handvatten. Binnen waterschapland is er nog te weinig hapklaar beschikbaar. Ieder vindt teveel het eigen wiel uit. Alle Overheden dienen te voldoen aan de BIO. Ik zou één overzichtelijke website willen (de bio-site) waarin de bio staat, maar ook beschikbare handleidingen en best practices, zodat het geen zoektocht is. Voorbeeld: hoofd HRM moet screeningsbeleid maken en implementeren. Dat kan al kant en klaar op de plank liggen en alleen te worden ingevoerd bij het waterschap...nu is het zoektocht.
Meer tijd en aandacht voor het onderwerp
Meer twee-richting verkeer, halen én brengen. IB vast onderwerp in agenda's bestuur.
Meer uitleggen wat er speelt, waar we rekening mee moeten houden, belang benadrukken zodat het onderwerp meer vragen oproept en er meer budget en tijd beschikbaar wordt gesteld.
Middelen
Moeilijk te zeggen aangezien ik pas sinds kort voor deze organisatie werk. De ervaring met mijn vorige werkgever is dat het belang van informatiebeveiliging weinig gezien wordt, en men vooral naar de euro's kijkt en niet inzien dat informatie en data ook een grondstof voor de bedrijfsvoering zijn. Door het openstellen van de CISO functie geeft men bij mijn huidige organisatie in ieder geval aan te willen investeren. De samenwerking met de bestuurder moet nog vorm gaan krijgen.

Moet ik nog gaan ervaren
Niet
Niet alleen sturen op rode kaarten, maar "permanent op de agenda"
niets
Niks, hele goede samenwerking
Nog beter vanuit de belevingswereld van de bestuurder een vertaling kunnen maken en het gesprek aan gaan.
Nog geen idee. Ikzelf ben net in dienst en informatiebeveiliging staat pas sinds kort echt op de agenda. Tot op heden is er een prima samenwerking
Noodzakelijkheden met bestuurlijke woorden niet kleiner maken en daardoor implementatie van maatregelen naar achteren schuiven.
op verschillende vlakken proactief adviseren i.p.v. ad hoc
Opname in allerlei bestaande cycli: - medewerkersbewustzijn in functioneringsgesprekken (als een kerncompetentie meenemen) - in (nu nog financiële) control-cyclus - opleiding en training personeel en studenten als standaard (in curriculum opnemen en als standaard opleiding voor (nieuwe) medewerkers)
Opnemen in de P&C cyclus
Periodiek overleg
Periodiek overleg.
Regelmatig overleg, dat ontbreekt nu
Regelmatiger overleg over stand van zaken
Regelmatiger overleg, betrokkenheid. Transparanter durven zijn naar gemeenteraad.
Regulier overleg, daadkrachtiger
Samenwerking met de portefeuillehouder werkt redelijk goed. Belangrijkere verbeterpunten zie ik bij directie en management
Samenwerking verloopt goed, op dit moment geen verdere verbetering noodzakelijk.
Structureel overleg
Structureler overleg
Toch nog wat meer aandacht en bewustwording voor dit onderwerp.
Uitwisselen van wederzijdse belangen en inzicht in risico's.
Vaker periodiek overleg
Van bij het begin betrokken worden bij nieuwe projecten/aankopen waar informatieveiligheid bij komt kijken.
Veel meer aandacht op dit dossier na de reorganisatie Nu ligt de focus vooral op de doorontwikkeling van de organisatie
Veel meer commitment.
Voer deze functie pas een week uit, dus dat kan ik nog niet zeggen
Voorbeeldfunctie van bestuur. Op dit moment is voornamelijk: Doe zoals ik zeg, maar niet zoals ik zelf doe.
Voorbeeldfunctie, ondersteunen van het belang van informatieveiligheid, lange termijn visie
Weinig. Samenwerking is prima.
Zie bovenstaande

Bijlage VI. Wat kan volgens de bestuurder verbeteren in de relatie met de CISO?

Wat zou kunnen verbeteren in de samenwerking met de CISO?
Aansluiting risicomanagement IB op risicomanagement van het hele instituut
ben tevreden over de samenwerking nu
Door krappe bezetting te veel tijd kwijt aan operatie en te weinig om meer beleidsmatig actief te zijn
Lijnmanager meer verantwoordelijk voor uitvoering; CISO meer in rol adviseur
Niet zo zeer met CISO, maar bewustzijn van organisatie kan groeien.
Niet zozeer een verbetering, maar wel 2 vraagstukken: - de balans tussen de CISO en de decentrale IB&P verantwoordelijkheden van de bedrijfsonderdelen. - IB&P meer als organisatievraagstuk zien i.p.v. technisch gedreven vanuit normenkaders
Beter zicht op de rol van de CSIO i.r.t. tot andere toezichthoudende rollen Meer zicht op incidenten en te nemen beheersmaatregelen
bewustwording dat de CISO rol adviserend is; maar dat management verantwoordelijk is
Integraal denke vanuit de belangen van inwoner en organisatie
Is in ontwikkeling en die ontwikkeling moeten we voortzetten
Korte lijn Gedeelde ambitie
Niets
Samenwerking is goed. We hebben veel aandacht voor het continu verbeteren van het inbedden van de nodige activiteiten rond informatieveiligheid in ons voortbrengingsproces.
Verstrekken van geanonimiseerde voorbeelden van aansprekende incidenten en de gevolgen daarvan
De CISO is een relatief nieuwe functie in de organisatie. Het moet nog in de genen van de gehele organisatie komen dat de CISO stelselmatig wordt betrokken bij ontwikkelingen waarbij informatieveiligheid een aandachtspunt is.
Geen verbeterpunten
Wellicht een grotere rol op organisatieverandering.
Zichtbaarheid
Op dit moment is er een vacature, dus n.v.t.
Pro-actiever aangeven wat wij zouden kunnen doen om onze informatiebeveiliging op een hoger niveau te brengen
Rolduidelijkheid
Structurele informatielijn, een dashboard met trends plus risico analyse
Werken aan bewustzijn binnen primaire proces Rolopvatting en mandaat binnen de organisatie
Daar kan ik nog geen antwoord op geven aangezien ik minder dan 3 maanden werkzaam ben voor deze organisatie.
Niet tussen de CISO en mij, wel tussen de CISO en de technische beheerclub
Regulier tijdstip afstemming in plaats van ad hoc
De samenwerking vormgeven vanuit heldere definities. Het hierboven gegeven rijtje mogelijke taakelementen geeft al aan dat de CISO net als de controller een containerbegrip dreigt te worden waar je alles in kunt kieperen. Daar is niemand bij gebaat. Behalve consultancy bureaus die gebruik maken van de verwarring en daar goed geld mee verdienen.
Ik ben zeer tevreden over onze CISO
Kennis onderhouden van de CISO afdeling omtrent nieuwe technologie.
Van belang is dat kleinere uitvoerders goed toegang hebben tot ontwikkelingen
CISO net aangesteld. Meer contact met onderzoeksteams en werkvloer om "practise what you preach" bij de organisatie te bevorderen.