

Marit Wensink

M&I/Partners

FORMATIEONDERZOEK INFORMATIEBEVEILIGING EN PRIVACY GEMEENSCHAPPELIJKE REGELINGEN 2025

ICT in perspectief

M&I/Partners/
adviseurs voor management en informatie

1 Managementsamenvatting

Hoe ziet informatiebeveiliging- en privacy-organisatie (IB&P) van gemeenschappelijke regelingen (GR'en) eruit? Al een aantal jaar voeren we het **formatieonderzoek gemeenten** uit. In 2025 hebben we ons onderzoek uitgebreid met gemeenschappelijke regelingen: hierbij ging het om Shared Service Centra (inclusief centrumgemeenten), Veiligheidsregio's, GGD'en en sociaal domein-organisaties.

Uit ons onderzoek blijkt dat GR'en basisinformatiebeveiligings- en privacyformatie hebben, maar dat deze vaak klein is. Ondanks die kleine formatie slagen ze er in een solide basis te leggen, met een CMMi-volwassenheidsniveau tussen 2 en 3. Tegelijkertijd komen er grote uitdagingen op hen af door geopolitieke ontwikkelingen en uitdijende wet- en regelgeving. Dit betekent dat organisaties meer werk moeten verzetten op het gebied van informatiebeveiliging en privacy, maar dat er niet persé meer middelen beschikbaar zijn.

Een aantal belangrijke bevindingen:

- SSC's scoren een hogere volwassenheid op IB&P-gebied dan centrumgemeenten, ondanks hun kleinere formatie.
- Hoewel Veiligheidsregio's en GGD'en onderling sterk verschillen in de gevoeligheid van hun dienstverlening, zijn de verschillen in formatie en volwassenheid minimaal.
- Sociaal domein-organisaties hebben de kleinste formatie van alle GR'en, terwijl ze veel gevoelige persoonsgegevens verwerken van inwoners. Zij hebben ook de meeste dubbelrollen.



Inhoud

1

Managementsamenvatting

2

Inleiding

3

IB&P bij SSC's en Centrumgemeenten

4

IB&P bij Veiligheidsregio's en GGD'en

5

IB&P bij sociaal domein-organisaties

6

Conclusie: IB&P bij GR'en

7

Onderzoeksmethodiek

8

Bijlagen

2 Inleiding

Hoe ziet de formatie van informatiebeveiliging en privacy in de overheid eruit? Is onze formatie vergelijkbaar met andere formaties? Wij hebben bepaalde dubbelfuncties, is dat wenselijk? En hoe verhouden onze ambities op privacy en informatiebeveiliging zich tot de formatie die we hebben?

Regelmatig ontvangen we bij M&I/Partners deze en vergelijkbare vragen. Om deze vragen goed te kunnen beantwoorden, is M&I/Partners in 2022 gestart met het [Formatieonderzoek privacy in de lokale overheid](#). We vroegen lokale overheidsorganisaties naar hun volwassenheidsniveau, ambities, formatie en groei-behoefte. In 2024 breidden we het onderzoek uit met het [Formatieonderzoek informatiebeveiliging](#). Ook dit jaar publiceerden we [de cijfers van de IB&P-organisatie in de gemeenten](#).

In 2025 breidden we ons onderzoek verder uit naar GR'en. Dit jaar publiceren we het tweede rapport over GR'en. Hierdoor kunnen we SSC's (inclusief centrumgemeenten), veiligheidsregio's, GGD'en en organisaties in het sociaal domein onderling vergelijken.

In de periode van 21 oktober tot en met 31 december verspreidden we de vragenlijst, met als doel organisaties te informeren over de trends van het afgelopen jaar.

De resultaten zijn opgedeeld in twee publicaties: één met de cijfers van gemeenten en één met de cijfers van GR'en. In deze publicatie kijken we naar de volwassenheid, ambities en (gewenste) formatie van GR'en.



IB&P bij SSC's en Centrumgemeenten

3 Over de deelnemers

Aan het onderzoek namen zowel Shared Service Centra als Centrumgemeenten deel.

- Shared Service Centra zijn GR'en, vaak georganiseerd in de vorm van een gemeenschappelijke regeling, waar gemeenten en andere GR'en ICT-diensten afnemen, soms aangevuld met andere diensten zoals personeel- en salarisadministratie of archivering.
- Centrumgemeenten zijn gemeentelijke organisaties die ICT-diensten leveren aan omliggende gemeenten. Hoewel ze geen GR'en zijn, zijn centrumgemeenten wel meegenomen in deze rapportage, vanwege hun belangrijke rol als samenwerkingspartner voor andere gemeenten. We verwachten dat hun ICT-dienstverlening, impact heeft op de formatiecijfers, met name op de informatiebeveiligingsformatie.

In de rest van dit rapport zijn de cijfers opgesplitst in deze twee categorieën. In totaal namen er **7 centrumgemeenten** en **6 SSC's** deel aan het onderzoek.

Om de gegevens vergelijkbaar te maken, is berekend aan hoeveel inwoners de SSC's en centrumgemeenten dienstverlening bieden (zoals staat beschreven in de vastgestelde regelingen). Dit is vervolgens omgerekend naar aantal fte per 100.000 inwoners.



3 IB&P bij SSC's en centrumgemeenten

Al sinds de inwerkingtreding van de AVG (2018) is privacy een aandachtspunt in gemeenteland. Ook de aandacht voor informatiebeveiliging gaat lang terug, naar de inwerkingtreding van de BIO en de daarvoor geldende BIG. Bij SSC's is de aandacht vaak pas later gekomen: vaak zijn deze organisaties opgericht met bepaalde dienstverlening als primaire focus (zoals ICT), en was de aandacht voor bedrijfsvoering minder aanwezig in de eerste jaren. Toch zien we de afgelopen jaren steeds meer aandacht voor privacy en informatiebeveiliging bij SSC's. Gemeenten stellen namelijk steeds meer vragen en eisen aan hun ketenpartners.

Centrumgemeenten profiteren van het feit dat zij al langer aandacht hebben voor informatiebeveiliging en privacy, maar ook zij krijgen te maken met ketenpartners (vaak kleinere gemeenten of GR'en) die vragen en eisen stellen.

Onze verwachtingen voorafgaand aan het onderzoek waren:

- elke SSC en centrumgemeente heeft een basisteam in huis: er zijn een FG, privacy officer en CISO/ISO aanwezig;
- centrumgemeenten zijn volwassener dan SSC's op zowel privacy als informatiebeveiliging, omdat zij ook voor hun verdere dienstverlening met deze onderwerpen bezig zijn;
- hoe groter de formatie, hoe volwassener de SSC/centrumgemeente op dat gebied;
- het ambitieniveau ligt hoger dan het volwassenheidsniveau, en parallel daaraan is er een groeibehoefte in formatie over de hele linie;
- de groeibehoefte zit vooral in de operationele rollen (TISO en PO, niet CISO/FG);
- 1 fte FG is een 'plafond', ongeacht organisatiegrootte;
- 1 fte CISO is een 'plafond', ongeacht organisatiegrootte;
- SSC's hebben minder privacyformatie in huis dan centrumgemeenten per 100.000 inwoners.

3 Volwassenheid & ambitie privacy

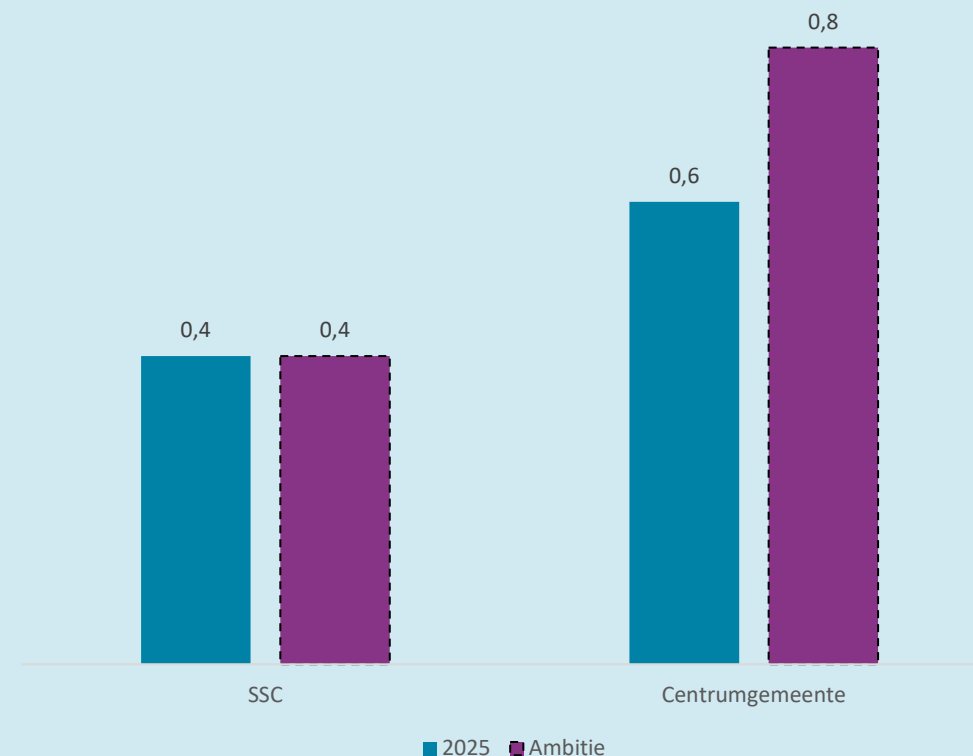
- Omdat bij centrumgemeenten al langer de aandacht op privacy gevestigd is, hadden we daar een hoger volwassenheidsniveau verwacht dan bij SSC's. Dit blijkt niet het geval: SSC's zijn zelfs iets volwassener op privacygebied dan centrumgemeenten.
 - Een mogelijke verklaring hiervoor is dat centrumgemeenten een stuk complexer zijn dan SSC's: naast ICT-dienstverlening en andere bedrijfsvoeringsprocessen, hebben zij vaak ook taken op het gebied van fysiek domein, sociaal domein en openbare orde en veiligheid. Hierdoor heeft privacy meer aandacht in deze organisaties. SSC's zijn ongeveer even volwassen als de gemeenten uit ons [formatieonderzoek IB&P gemeenten 2025](#).
- Met name SSC's hebben een hoog ambitieniveau geformuleerd, met een stijging van maar liefst 1,4 punt naar net onder [het CMMi-niveau](#) beheerst. Centrumgemeenten hebben ook een groeibehoefte, maar die ligt iets lager.



Grafiek 1 Gemiddelde volwassenheid privacy conform het CMMi-model, gesplitst naar centrumgemeenten en SSC's

3 Formatie privacy: de FG

- In lijn met onze verwachting rapporteerden alle deelnemende SSC's en centrumgemeenten dat zij een FG hadden aangesteld.
- Per 100.000 inwoners lag de FG-formatie van SSC's lager dan bij centrumgemeenten.
 - De meest waarschijnlijke verklaring hiervoor is dat er minder gegevensverwerkingen zijn bij SSC's, waardoor de FG minder tijd hoeft te besteden aan diens taken.
- Interessant genoeg lijkt inwoneraantal geen invloed te hebben op de formatie van FG bij SSC's: kleinere SSC's hadden soms een grotere absolute formatie dan grote SSC's.
- Bij centrumgemeenten was dit wél het geval: een grotere hoeveelheid inwoners hangt samen met een hogere FG-formatie.
- SSC's hadden een minimale groeibehoefte: zij zijn erg tevreden over hun FG-formatie.

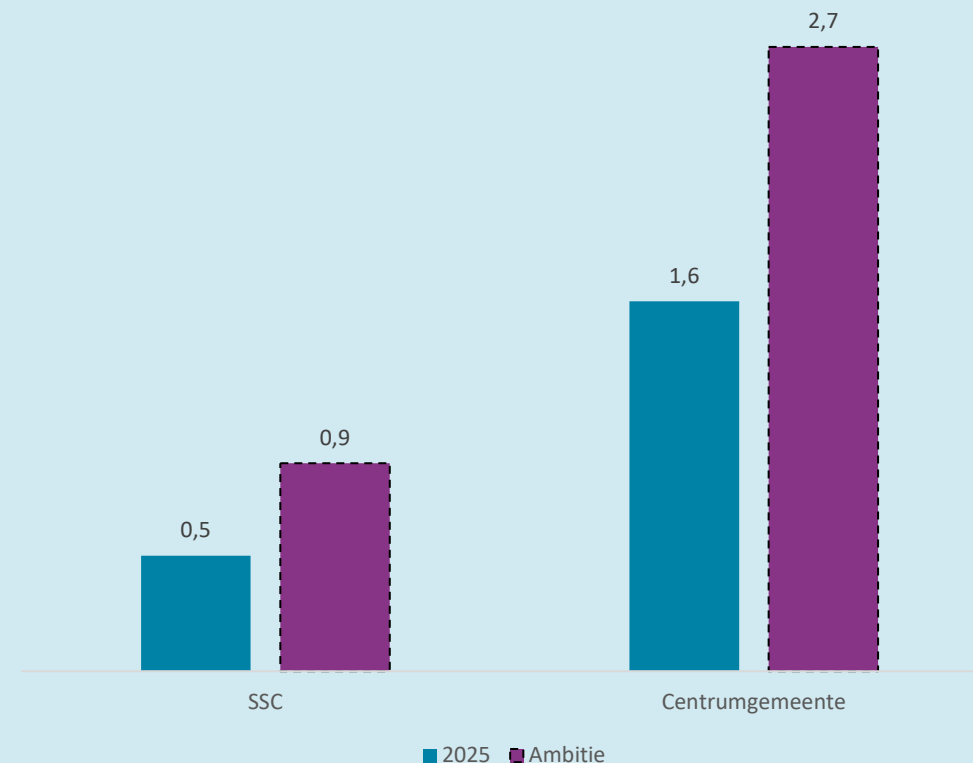


Grafiek 3 Gemiddelde formatie van de functionaris gegevensbescherming per 100.000 inwoners en de ambitie voor komende periode, gesplitst naar SSC's en centrumgemeenten.

3 Formatie privacy: de privacy officer

Elke organisatie had een privacy officer, zoals we hadden verwacht.

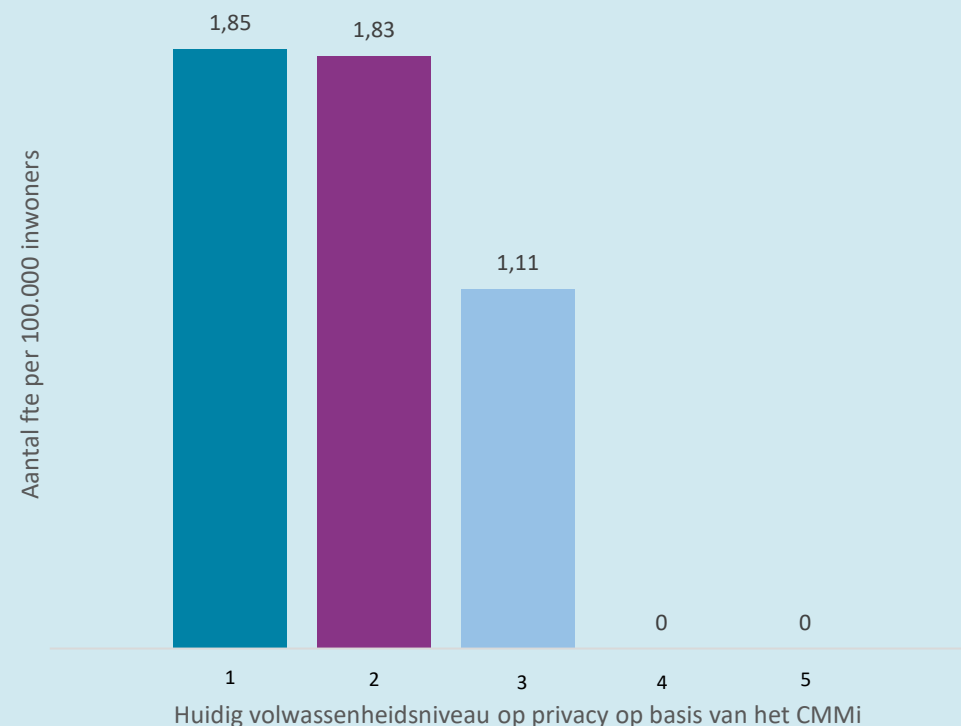
- Er zijn wel grote verschillen in de hoeveelheid fte's: de aantallen liepen tussen de 0,2 en 4 fte.
 - SSC's hebben zowel relatief als absoluut een veel lagere privacy officer-formatie.
 - Ook hier geldt dat de hoeveelheid gegevensverwerkingen waarschijnlijk een logische verklaring is voor de formatieverschillen. Inwonersaantal was opnieuw geen bepalende factor: een grotere SSC had niet altijd meer formatie dan een kleinere SSC.
- In tegenstelling tot de FG-rol hebben SSC's wél een behoefte om te groeien in de privacy officer-formatie: per 100.000 inwoners willen ze bijna verdubbelen.
- Centrumgemeenten hebben een iets kleinere groeibehoefte, van ruim 1,1 fte per 100.000 inwoners.



Grafiek 4 Gemiddelde formatie van de privacy officer per 100.000 inwoners en de ambitie voor komende periode, gesplitst naar SSC's en centrumgemeenten.

3 Relatie tussen privacyvolwassenheid en teamgrootte

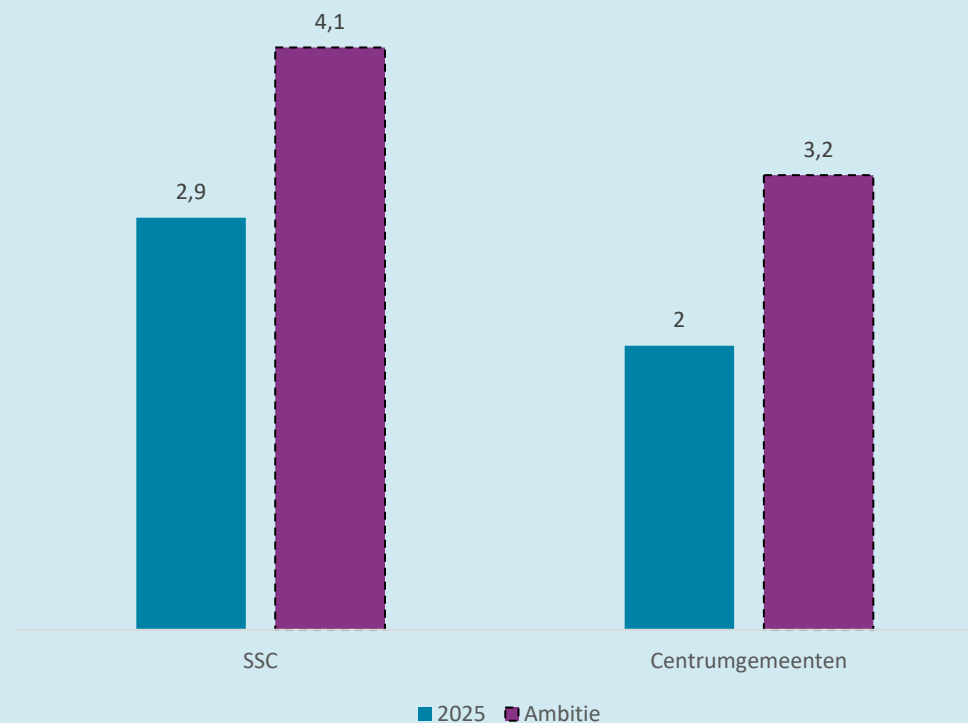
- Er is geen duidelijke samenhang tussen de privacyvolwassenheid van een SSC of centrumgemeente en de grootte van het privacyteam. De verschillen zijn klein, waarbij een volwassener organisatie (CMMi-niveau 3) een iets kleiner team had dan een organisatie op het laagste volwassenheidsniveau (respectievelijk 1,11 en 1,85 fte per 100.000 inwoners).
- We keken ook of er een samenhang is tussen de privacyambitie (de behoefte om te groeien in privacyvolwassenheid) en de behoefte om het team uit te breiden. Hier was geen duidelijk verband te zien: teams met een grotere volwassenheidsambitie hadden niet een grotere groei-behoefte.



Grafiek 7 Gemiddelde fte van het totale privacyteam per 100.000 inwoners, gesplitst naar gerapporteerd volwassenheidsniveau. Eén organisatie rapporteerde volwassenheidsniveau 4 en is vanwege herleidbaarheid verwijderd uit deze grafiek.

3 Volwassenheid & ambitie informatiebeveiliging

- In lijn met onze verwachtingen is de volwassenheid van SSC's op informatiebeveiligingsgebied hoger dan op [privacygebied](#). Het verschil is niet groot: 0,4 punt.
- Opnieuw rapporteren centrumgemeenten een lager volwassenheidsniveau dan SSC's.
 - Net als bij privacy kan het zo zijn dat de complexiteit van de organisatie bijdraagt aan een lager volwassenheidsniveau.
 - Daarnaast hebben SSC's het leveren van ICT-diensten vaak als *core business*. Mogelijk dat zij daardoor een betere focus hebben op informatiebeveiliging.
- Beide typen organisaties formuleerden een forse ambitie: ze willen de komende periode gemiddeld met 1,2 punt toenemen in volwassenheid, van niveau 2/3 naar niveau 3/4 op [het CMMi](#).



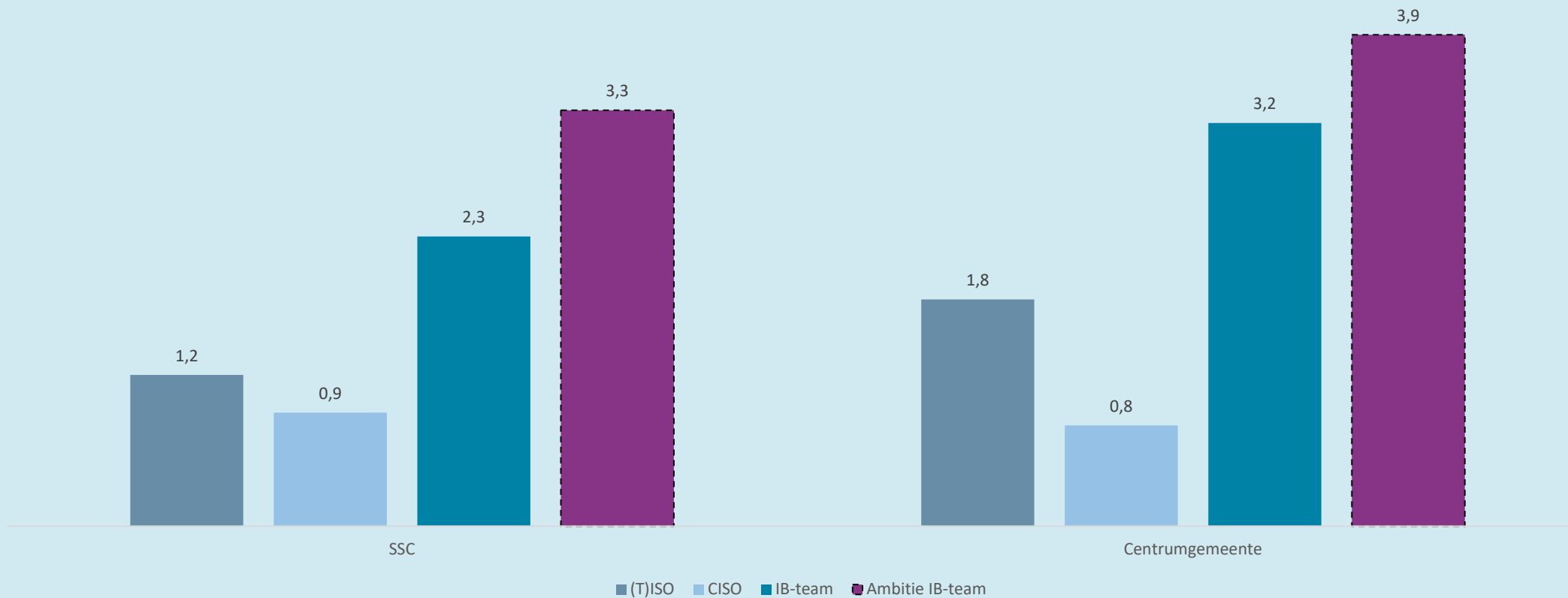
Grafiek 5 Volwassenheid informatiebeveiliging conform het CMMi-model, gesplitst naar centrumgemeenten en SSC's

3 Formatie Informatiebeveiliging

Onze verwachting dat elke SSC en centrumgemeenten een CISO of ISO had aangesteld, klopt. Op de volgende pagina worden de cijfers in één grafiek gepresenteerd. Een aantal opvallende bevindingen:

- SSC's hebben een duidelijke 'vloer' van CISO-fte: elke SSC had minimaal 1 fte CISO tot maximaal 2 fte. Dit is anders dan we op voorhand dachten: we verwachtten dat er wel een 'plafond' zou zijn, niet persé een 'vloer'. Bij centrumgemeenten is er wat meer variatie; zij hadden regelmatig minder dan 1 fte CISO in dienst (tussen de 0,5 en 1,5 fte).
- SSC's bedienen een grotere groep inwoners dan centrumgemeenten, maar relatief gezien hebben ze bijna evenveel CISO-formatie als centrumgemeenten (0,8 vs. 0,9 fte per 100.000 inwoners).
- Er is enorm veel variatie in de hoeveelheid fte (T)ISO-functie die organisaties vermelden. Bij SSC's is er een direct verband te zien tussen inwoneraantal: hoe hoger het aantal inwoners, hoe groter de (T)ISO-functie. Bij centrumgemeenten blijkt dit verband verrassend genoeg niet.
- We vroegen naar de complete formatie van het IB-team. Bij centrumgemeenten bestond het IB-team meestal uit de totale som van CISO + (T)ISO. SSC's rapporteren vaker extra functies, zoals technische ondersteuning (o.a. SOC-diensten) en expertise op het gebied van business continuity management.
- Vrijwel alle organisaties gaven aan een groeiambitie te hebben. Zij hadden vooral behoefte aan uitbreiding van de 'klassieke' rollen, zoals CISO, ISO en TISO. Ook expertise op AI en Identity Access Management werd genoemd.

3 Formatie IB-team per 100.000 inwoners



Grafiek 6 Gemiddelde formatie van de CISO, (T)ISO en het complete IB-team, en de ambitie voor de komende periode gesplitst naar SSC's en centrumgemeenten.

Dubbelrollen

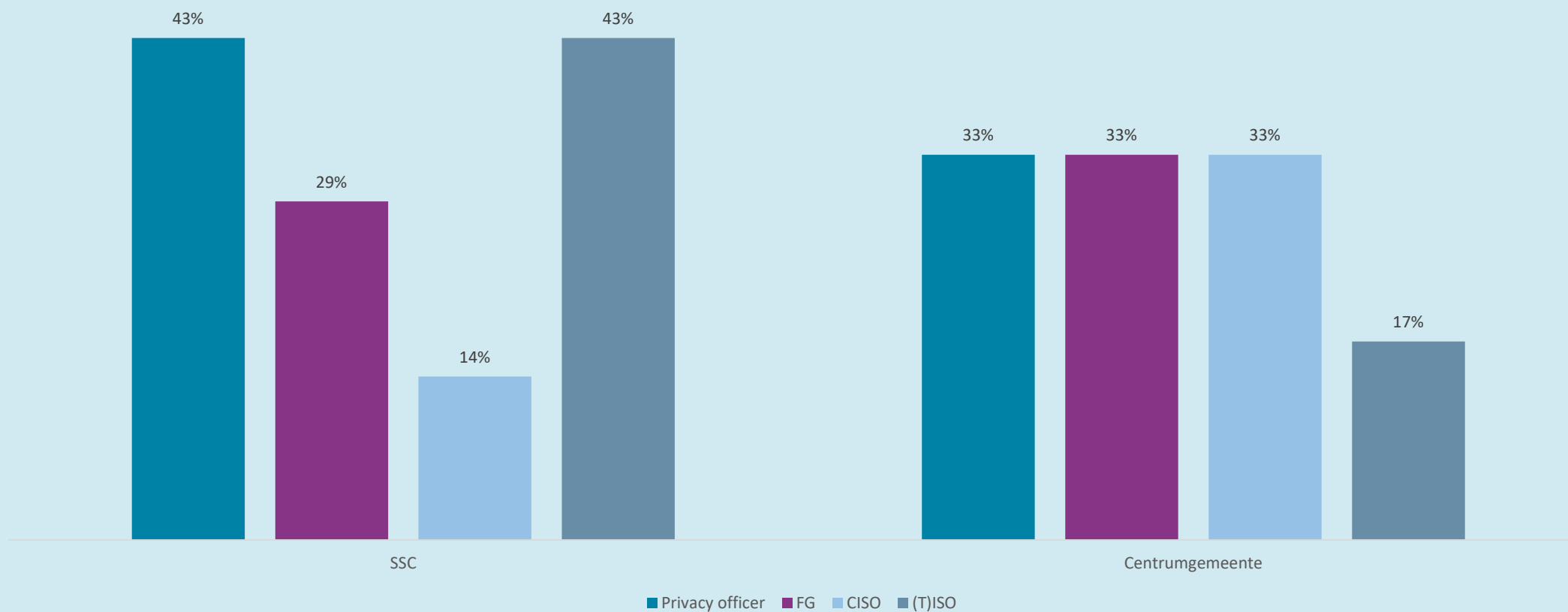
Dubbelrollen komen veel voor bij SSC's en centrumgemeenten. 77% van de deelnemende organisaties (10 van de 13) rapporteerde minimaal één dubbelrol. Zoals te zien op de volgende pagina, komen dubbelrollen bij alle uitgevraagde functies voor.

- Met name privacy officers hebben veel verschillende dubbelrollen. Vaak zijn ze verantwoordelijk voor een breder palet van 'compliance': ze zijn bijvoorbeeld ook verantwoordelijk voor de WPG, zijn security officer of spelen een rol rondom de AI-wetgeving in de organisatie.
- Ook FG's hebben variërende dubbelrollen. Juridisch adviseur komt het vaakst voor, maar er is ook een FG die tevens een ISO-functie bekleed.
- CISO's met een dubbelrol zijn vaak beleidsadviseur. Eén team rapporteerde dat de CISO tevens teamleider was.
- ISO's combineren hun werkzaamheden vaak met privacy officer-werkzaamheden.

Het feit dat dubbelrollen zoveel voorkomen, laat zien dat centrumgemeenten en SSC's vaak geen middelen vrij (weten te) maken om volwaardige functies te creëren: vaak heeft één persoon binnen de organisatie meerdere petten op. Hoewel de meest genoemde combinaties in zichzelf niet direct problematisch zijn, kan het bekleden van meerdere rollen in één organisatie uitdagend zijn. Het is de vraag of één medewerker in staat is voldoende tijd vrij te maken voor *alle taken* die die persoon heeft vanuit de verschillende rollen.



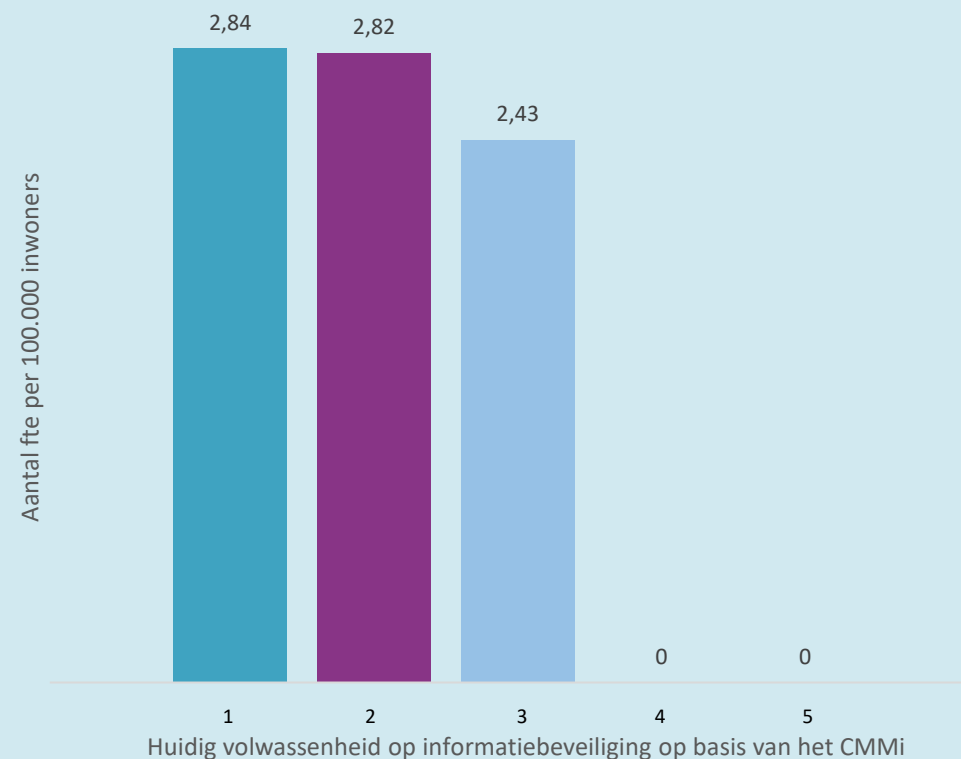
3 Percentage dubbelrollen



Grafiek 7 Percentage van functies die ook een dubbelrol vervullen, gesplitst naar SSC en centrumgemeenten

3 Samenhang tussen IB-volwassenheid en teamgrootte

- Er is geen duidelijke samenhang tussen de IB-volwassenheid van een SSC of centrumgemeente en de grootte van het IB-team. De verschillen zijn klein, waarbij een volwassenere organisatie ([CMMi-niveau 3](#)) een iets kleiner team had dan een organisatie op het laagste volwassenheidsniveau (respectievelijk 2,83 en 2,43 fte per 100.000 inwoners).
- We keken ook of er een samenhang is tussen de IB-ambitie (de behoefte om te groeien in IB-volwassenheid) en de behoefte om het team uit te breiden. [Net als bij privacy](#) geldt dat er hier geen duidelijk verband te vinden is.



Grafiek 8 Gemiddelde fte van het totale privacyteam per 100.000 inwoners, gesplitst naar gerapporteerd volwassenheidsniveau. Eén organisatie rapporteerde volwassenheidsniveau 4 en is vanwege herleidbaarheid verwijderd uit deze grafiek.

3 Conclusie: IB&P bij SSC's en Centrumgemeenten

- SSC's en centrumgemeenten zijn nog **kwetsbaar** als het gaat om privacy en informatiebeveiliging. Het gemiddelde volwassenheidsniveau van beide typen organisaties op privacy en informatiebeveiliging stijgt nog niet uit boven 'herhaalbaar' of 'gedefinieerd' conform [het CMMi](#), terwijl gedefinieerd het minimumstreven moet zijn. SSC's zijn iets volwassener dan centrumgemeenten, waarschijnlijk omdat zij vaak minder processen en gegevensverwerkingen hebben, en zich mede daardoor in een minder complex speelveld bevinden.
- Zowel SSC's als centrumgemeenten hebben een hoge ambitie, zowel voor privacy als voor informatiebeveiliging. De formatie matcht echter niet met de ambitie: er is soms een zeer minimale rolinvulling. Zo hebben SSC's [een lage PO-formatie](#) (0,5 fte per 100.000 inwoners), en bekleedt deze PO vaak [een dubbelrol](#).
- Tegelijkertijd lijkt een groter team [geen garantie](#) voor een hoger volwassenheidsniveau. Mogelijk investeren deze organisaties in een groter team, omdat ze worstelen met achterstand en deze weg willen werken. Daarnaast is het belangrijk om informatiebeveiliging en privacy niet enkel bij specialisten te beleggen: als privacy en informatiebeveiliging niet gedragen worden door de gehele organisatie, zal de impact van het privacy- en IB-team altijd beperkt blijven. Dat kan de weerbaarheid van deze organisaties onder druk zetten.
 - Met de Cyberbeveiligingswet in aantocht kunnen bestuurders er niet meer omheen: ze zullen informatiebeveiliging en privacy serieus moeten nemen als een organisatorisch vraagstuk.

IB&P bij Veiligheidsregio's en GGD'en

4 Over de deelnemers

- Veiligheidsregio's (VR'en) en Gemeentelijke Gezondheidsdiensten (GGD'en) voeren namens de gemeenten in hun regio een aantal wettelijke taken uit. Voor de Veiligheidsregio's zijn deze vastgelegd in de **Wet Veiligheidsregio's**, voor GGD'en (veelal) in de **Wet publieke gezondheid**. Gemeenten besteden dus taken uit aan deze gemeenschappelijke regelingen.
 - Het wisselt vaak welke taken er exact onder een VR en GGD vallen: zo hebben sommige VR'en ook ambulancediensten of een meldkamer, andere niet. GGD'en hebben vaak variaties in de details van de dienstverlening: zo levert vrijwel elke GGD jeugdgezondheidszorg, maar voor verschillende doelgroepen (denk aan wel/geen consultatiebureaus).
 - Er is vaak intensieve samenwerking tussen de Veiligheidsregio's en GGD'en. Soms zijn deze zelfs georganiseerd in één gemeenschappelijke regeling. Daarom publiceren we de cijfers van deze organisaties in één overzicht.

- In totaal namen er 13 GGD'en en VR'en deel aan het formatieonderzoek. Dit betrof: 5 zelfstandige GGD'en, 2 Veiligheidsregio's met een GGD, en 6 Veiligheidsregio's zonder GGD. Van die laatste groep verwerkten 4 VR'en wel gezondheidsgegevens, bijvoorbeeld omdat ze een meldkamer of ambulancedienst als organisatieonderdeel hadden.

- Om herleidbaarheid van de cijfers te voorkomen én de cijfers zo goed mogelijk vergelijkbaar te maken, houden we de volgende verdeling aan:

Categorie	Aantal deelnemers
GGD of VR met GGD	7
Veiligheidsregio zonder GGD	6

4 IB&P bij VR'en en GGD'en

Bij GGD'en heeft de IB&P-organisatie sinds de COVID-pandemie een behoorlijke boost gekregen, niet alleen gedurende de coronacrisis maar ook daarna. GGD'en kregen veel taken onder hoge druk op hun bordje, maar kwamen ook op [de radar van toezichthouders](#). Ze hebben daarom sinds 2020 veel in privacy en informatiebeveiliging geïnvesteerd. GGD'en moeten zich houden aan de NEN7510.

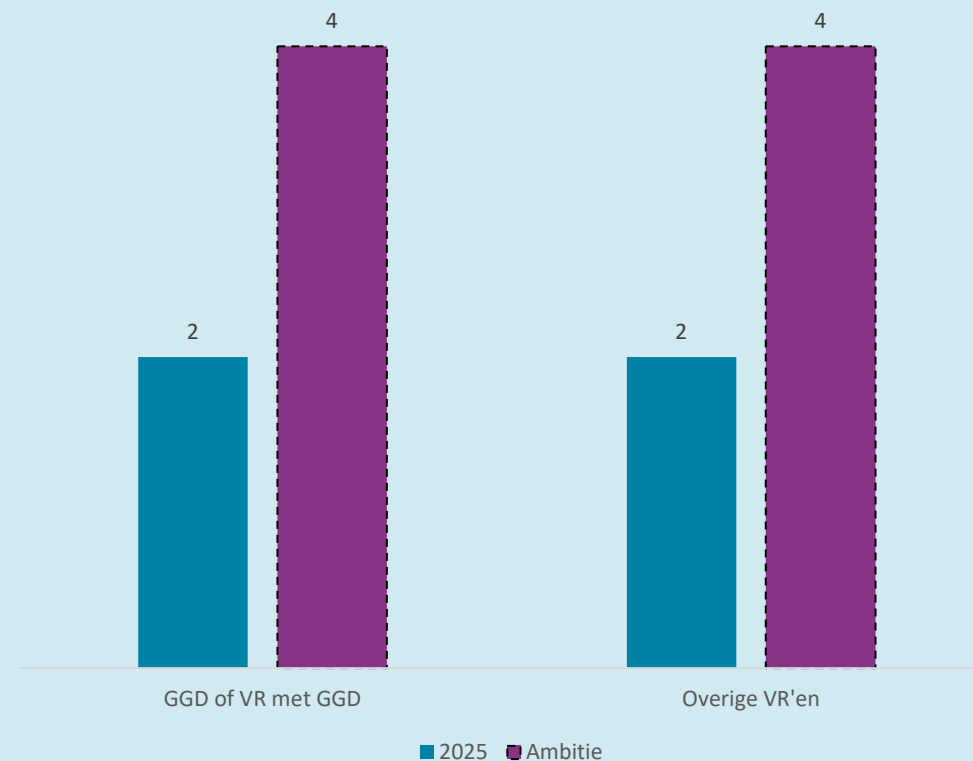
Veiligheidsregio's zijn onderdeel geweest van het [Versnellingsprogramma Informatieveiligheid](#), wat een positief effect had op hun IB-volwassenheid. Veiligheidsregio's die gezondheidsgegevens verwerken, moeten ook voldoen aan de NEN7510; voor Veiligheidsregio's met een ambulancedienst is certificering tegen de norm zelfs [verplicht](#).

Onze verwachtingen waren:

- elke VR en GGD heeft een basisteam in huis: er zijn een FG, privacy officer en CISO/ISO aanwezig;
- hoe groter de formatie, hoe volwassener de organisatie op dat gebied;
 - Veiligheidsregio's zijn volwassener in informatiebeveiliging dan in privacy en hebben hier ook meer formatie op.
 - GGD'en zijn volwassener in privacy dan informatiebeveiliging en hebben hier ook meer formatie op.
- de groeibehoeft zit vooral in de operationele rollen (TISO en PO, niet CISO/FG);
- 1 fte FG is een 'plafond', ongeacht organisatiegrootte;
- 1 fte CISO is een 'plafond', ongeacht organisatiegrootte;
- Organisaties die ICT uitbesteden, hebben minder technische kennis in huis en zijn meer een regie-organisatie.

4 Volwassenheid & ambitie privacy

- In tegenstelling tot onze verwachting, was er geen verschil tussen Veiligheidsregio's met GGD en zelfstandig GGD'en ten opzichte van overige VR'en: beide rapporteerden hetzelfde gemiddelde volwassenheidsniveau.
 - Een mogelijke verklaring is dat Veiligheidsregio's zonder GGD vaak minder persoonsgegevens verwerken, waardoor zij sneller een vergelijkbaar volwassenheidsniveau bereiken.
- Tegelijkertijd toont dit ook aan dat er nog erg veel werk aan de winkel is: volwassenheidsniveau 2 is erg laag.
 - Beide groepen tonen zich gelukkig ambitieus: ze willen de komende periode naar [CMMi-niveau](#) *bestuurd*.



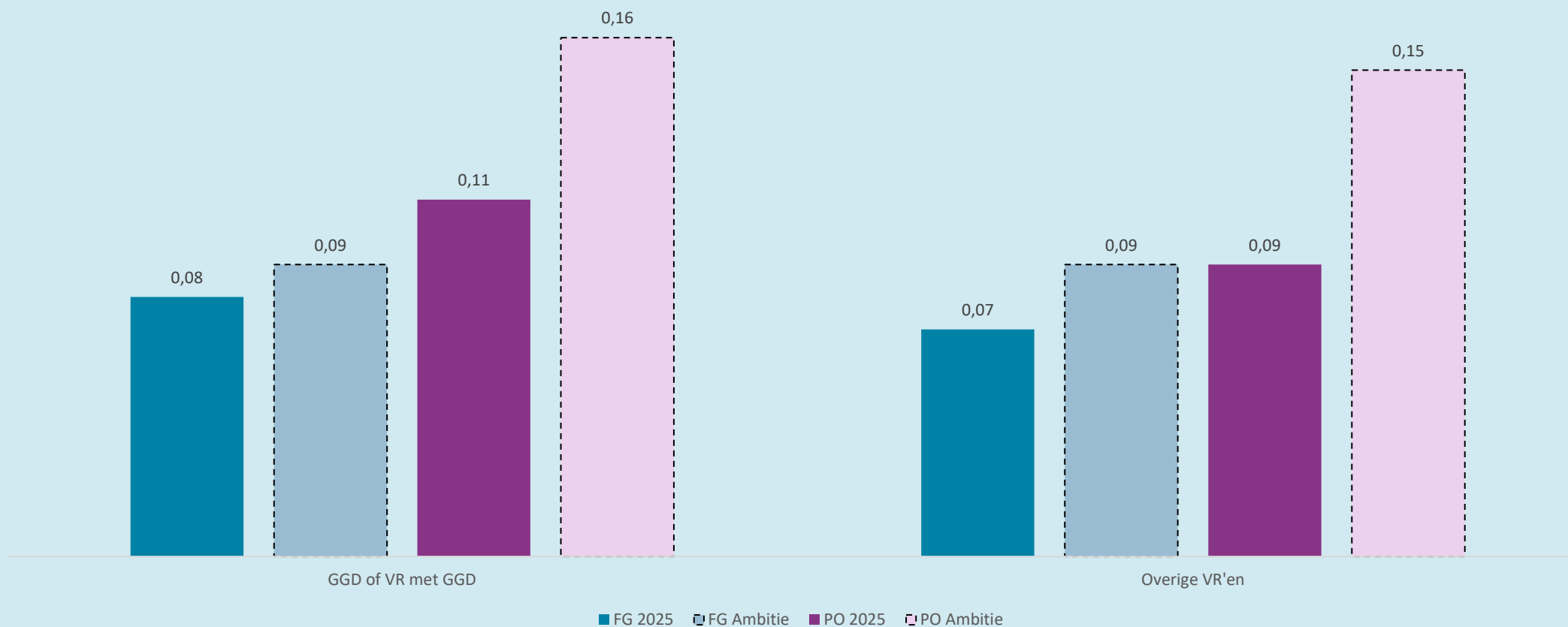
Grafiek 9 Gemiddelde volwassenheid privacy conform het CMMi-model, gesplitst naar organisatietype.

4 Formatie privacy

- Net als in het formatieonderzoek bij gemeenten is een duidelijk plafond zichtbaar: VR'en en GGD'en hebben maximaal één fte FG. De grafiek is zichtbaar op de volgende pagina.
 - Omdat GGD'en en VR'en grote groepen inwoners bedienen, zijn de relatieve FG-cijfers erg laag. In de praktijk was er veel variatie in de formatie van FG: tussen de 0,1 en 1 fte.
 - Er was geen duidelijke samenhang tussen de grootte van de VR/GGD en de FG-formatie.
- De privacy officer-formatie is iets groter dan de FG-formatie. In absolute aantallen varieerde deze van 0,33 tot 1,5 fte.
 - Ook hier geldt dat er geen duidelijke samenhang was tussen organisatiegrootte en hoeveelheid fte.
- De verschillen tussen de typen organisaties blijken klein, hoewel we verwachtten dat VR'en met GGD en zelfstandige GGD'en meer privacyformatie zouden hebben.
- Er was ook geen duidelijk samenhang tussen volwassenheid en teamgrootte of tussen ambitie en groei-behoefte.
- Beide groepen willen zowel groeien in PO- als in FG-formatie, maar de focus ligt wel op de operationele rol: daar willen Veiligheidsregio's en GGD'en harder in groeien dan in hun FG-formatie.



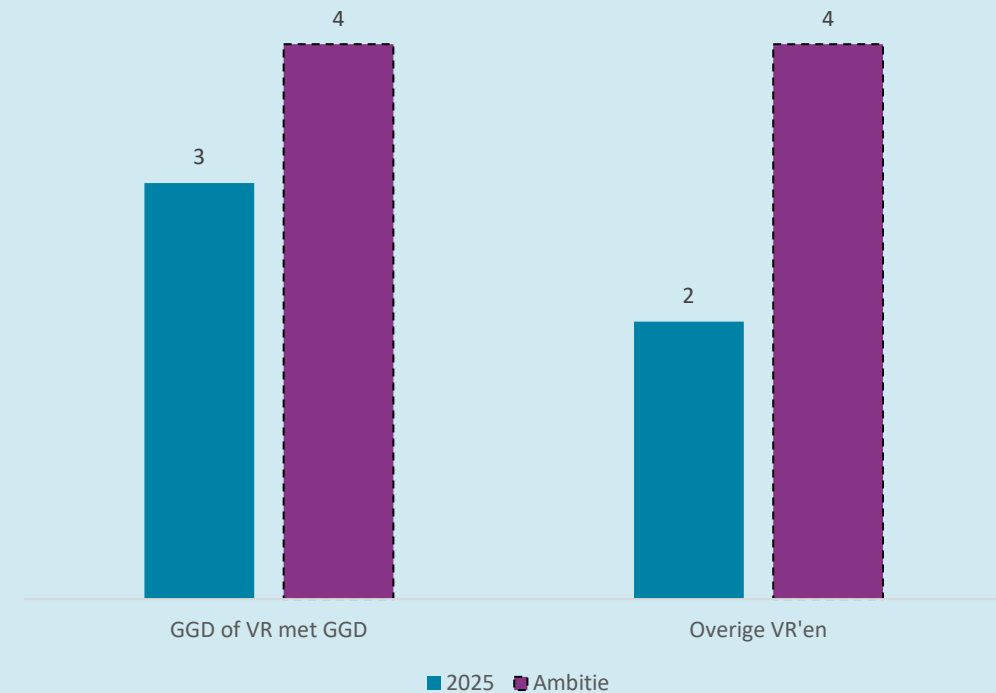
4 Formatie privacy



Grafiek 10 Gemiddelde formatie van de functionaris gegevensbescherming en privacy officer per 100.000 inwoner en de ambitie voor komende periode, gesplitst naar organisatietype.

4 Volwassenheid & ambitie IB

- In tegenstelling tot onze verwachting waren Veiligheidsregio's zonder GGD minder volwassen op informatiebeveiliging dan VR'en met GGD of zelfstandige GGD'en.
 - Uit de ruwe data blijkt zelfs dat GGD'en de meest volwassen organisaties zijn op IB: zij scoorden gemiddeld een 3,6, terwijl VR'en gemiddeld niet hoger scoorden dan 2,5.
 - Dit is opvallend, omdat Veiligheidsregio's een Versnellingsprogramma hadden om hun informatiebeveiliging te verbeteren.
- Net als bij [privacy](#) is er een hoge ambitie bij alle organisaties: beide groepen willen [het CMMi-niveau bestuurd](#) bereiken.



Grafiek 11 Gemiddelde volwassenheid informatiebeveiliging conform het CMMi-model, gesplitst naar organisatietype.

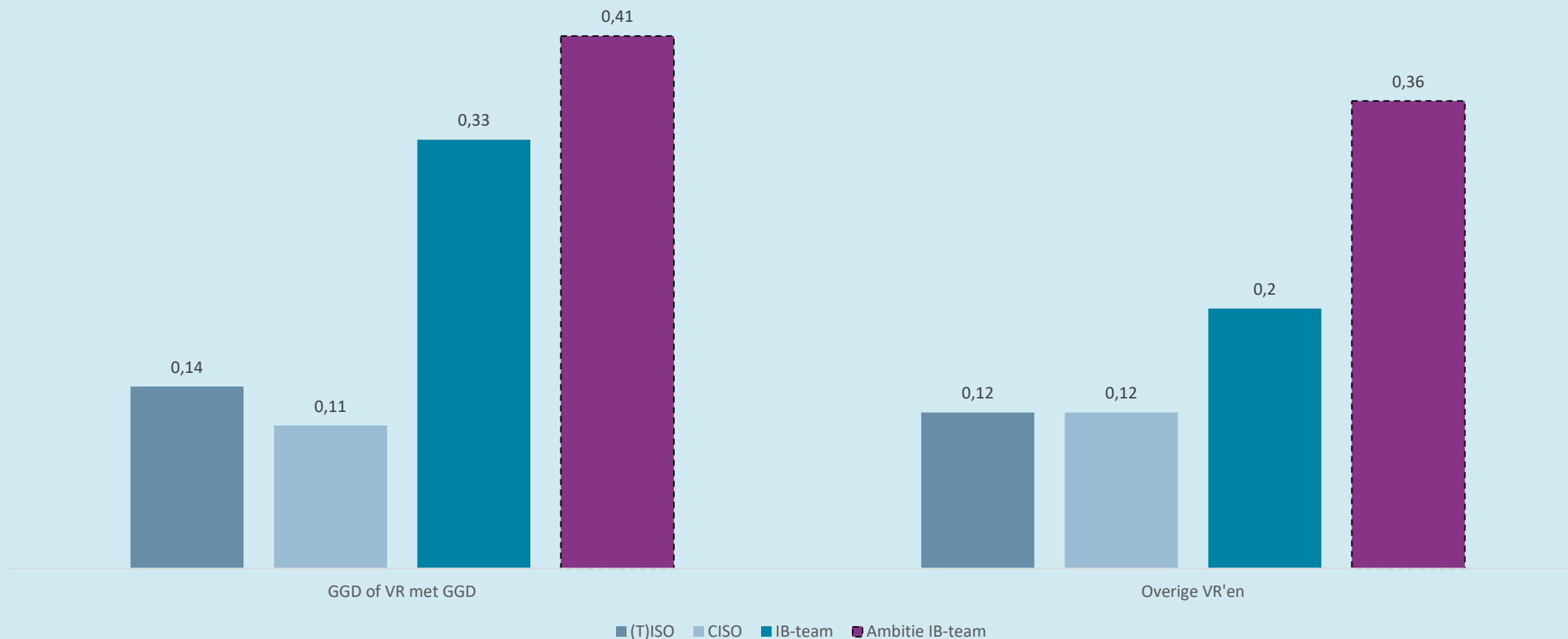
4 Formatie

Informatiebeveiliging

- In lijn met de verwachting is er een duidelijk plafond van 1 fte voor de CISO-functie. Slechts één organisatie meldde geen CISO-formatie te hebben. Verder hadden alle organisaties minimaal 0,5 fte CISO in dienst. Per 100.000 inwoners waren de verschillen tussen VR'en met GGD en zelfstandige GGD'en minimaal ten opzichte van overige Veiligheidsregio's.
- Er is veel variatie in de (T)ISO-functie. Twee VR'en meldden helemaal geen operationele informatiebeveiligingsrol te hebben; verder varieerde de formatie tussen 0,5 en 2,5 fte.
- Bij de meeste organisaties bestaat het IB-team enkel uit de optelsom CISO + (T)ISO. Slechts 4 organisaties (30%) meldden dat zij extra functies hadden binnen het IB-team. Dit zijn veelal technische rollen, zoals ICT-adviseur en IT-architecten.
 - Het betrof hier wel VR'en met een GGD of zelfstandige GGD'en: dit lijkt in lijn met het feit dat zij ook [volwassener zijn](#) op IB-gebied.
- Alle organisaties gaven aan een groeiambitie te hebben in hun IB-formatie. De gewenste groei zit veelal in de klassieke rollen: organisaties willen (extra of geformaliseerde) CISO's of ISO's in hun team opnemen. Verder werden ook rollen in business continuity management en riskmanagement als extra functies benoemd, mogelijk vanwege de extra aandacht die ligt op deze onderwerpen door geopolitieke ontwikkelingen en veranderingen in wet- en regelgeving.



4 Formatie IB-team per 100.000 inwoners

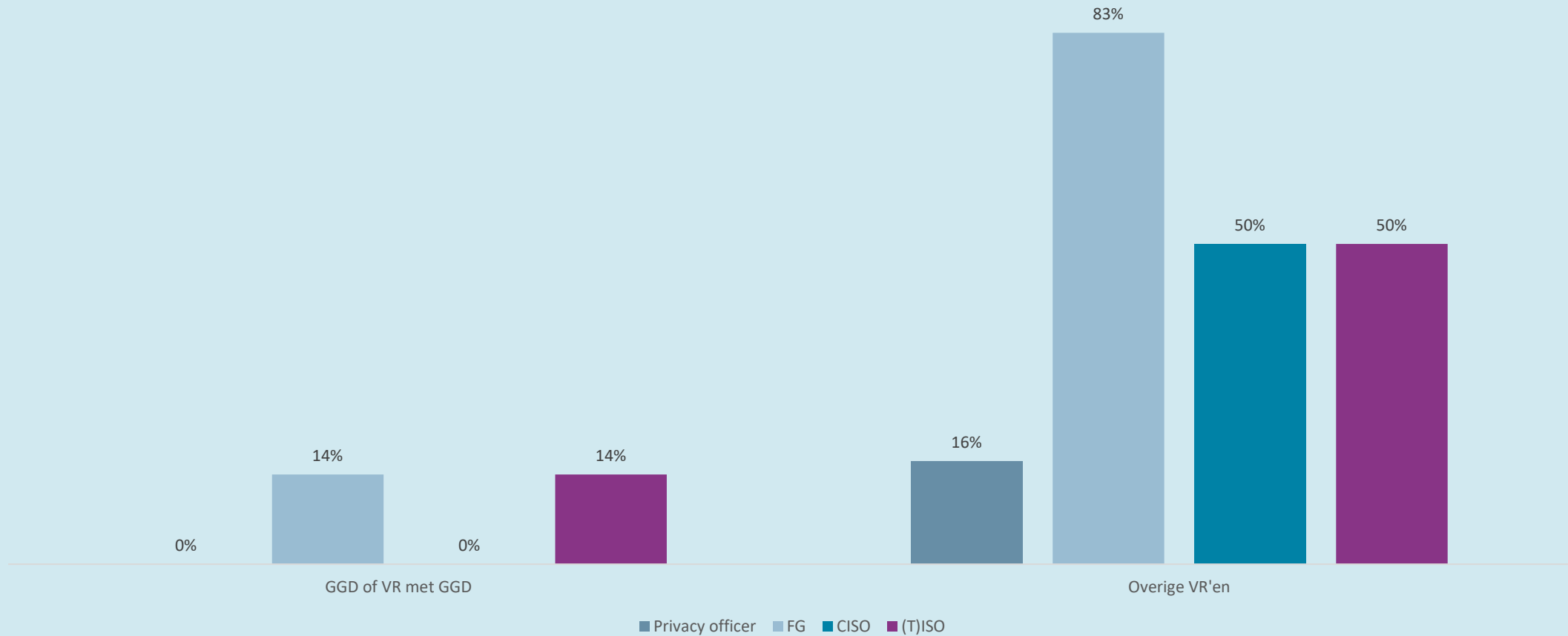


Grafiek 12 Gemiddelde formatie van de CISO, (T)ISO en het complete IB-team, en de ambitie voor de komende periode, gesplitst naar organisatietype.

4 Dubbelrollen

- Veiligheidsregio's met GGD en zelfstandige GGD'en rapporteerden veel minder dubbelfuncties dan de overige Veiligheidsregio's. Dit indiceert dat de eerste groep vaak in staat is volwaardige, losse functies te organiseren en dat werkzaamheden niet hoeven te worden gecombineerd met andere taken. Mogelijk heeft dit te maken met de urgentie die op dit onderwerp wordt ervaren, omdat zij (meer) gevoelige persoonsgegevens hebben.
- Bij Veiligheidsregio's zonder GGD had met name de Functionaris Gegevensbescherming opvallend vaak een dubbelrol. Bij één organisatie werden zelfs 4 andere rollen vermeld.
 - Over het algemeen waren de rollen wel verenigbaar met elkaar: FG's waren vaak juridisch adviseur of klachtencoördinator, rollen die niet inherent botsen met de onafhankelijke toezichtstaken van de FG.
 - Bij slechts één organisatie waren de rollen niet verenigbaar: de FG was onder andere ook privacy officer. Hierbij ontstaat ongewenste vermenging van de verschillende lijnen van [het three lines model](#).
- Slechts één organisatie vermeldde dat hun privacy officer een dubbelrol had: deze combineerde diens taken met een informatiebeveiligingsfunctie.
- In een paar gevallen combineerde de CISO diens functie met leidinggevende taken. Ook hier is er een mogelijk risico dat taken in [het three lines model](#) door elkaar raken: de CISO-functie is over het algemeen een tweede- of derdelijnsfunctie, terwijl een leidinggevende vaak vanuit de eerste lijn managementbeslissingen neemt.
- De (T)ISO combineerde diens werk vaak met meer technische functies.

4 Percentage dubbelrollen

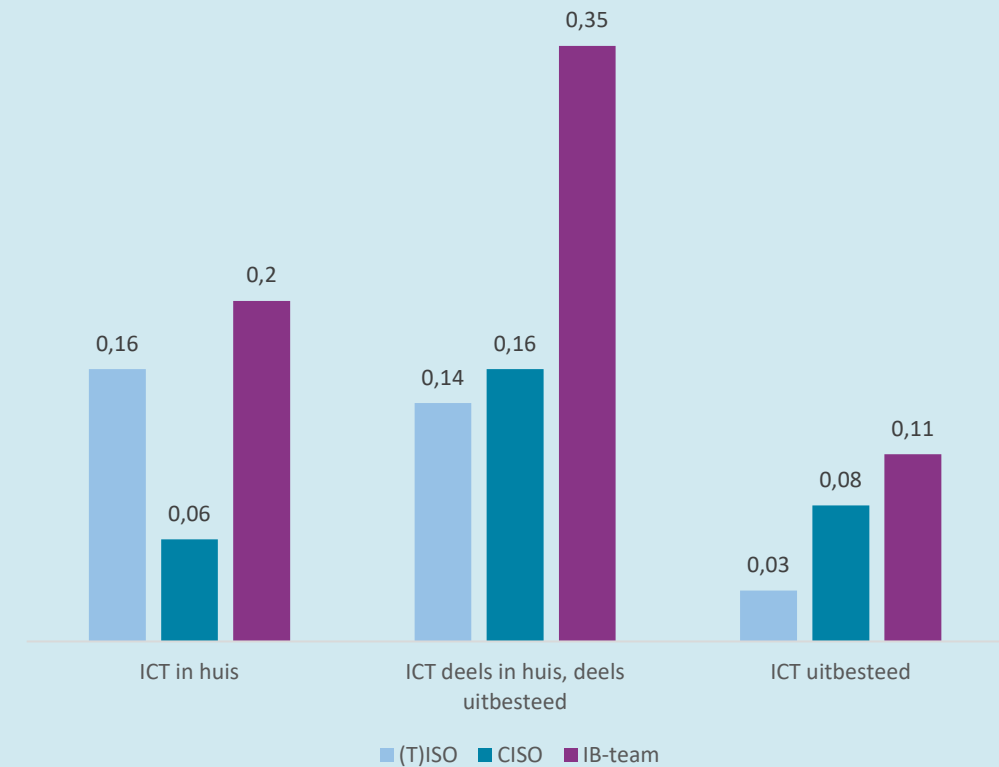


Grafiek 13 Percentage van functies die tevens een dubbelrol vervuld, gesplitst naar organisatietype.

ICT-regie

Onze verwachting was dat de verdeling van ICT-functies tussen organisaties zou verschillen, afhankelijk van ICT-inrichting.

- Uit ons onderzoek blijkt inderdaad dat VR'en en GGD'en die ICT zelf (deels) in huis hebben, een grotere (T)ISO-functie hebben.
- In tegenstelling tot wat we hadden verwacht, hadden organisaties die ICT uitbesteed hadden, niet een grotere CISO-functie; wel hadden ze in totaal een kleiner IB-team.
 - Dit is opvallend, omdat ook bij uitbesteding van ICT-regie op (technische) informatiebeveiliging belangrijk is. De CISO zou deze regiefunctie op zich kunnen nemen.
- Organisaties die ICT deels in huis hadden en deels uitbesteed, hadden de grootste IB-formatie. Een mogelijke verklaring is dat deze combinatie van ICT ervoor zorgt dat zij een meer complexe ICT-omgeving hebben, en daarom meer formatie nodig hebben.



Grafiek 14 Gemiddelde formatie van (T)ISO, CISO en het totale IB-team per 100.000 inwoners, gesplitst naar ICT-inrichting.

4 Conclusie: IB&P bij VR'en en GGD'en

- De afgelopen jaren hebben VR'en en GGD'en, mede door externe impulsen, een professionaliseringslag in informatiebeveiliging en privacy gemaakt.
 - Verrassend genoeg zijn juist [GGD'en volwassen in informatiebeveiliging](#), ondanks het Versnellingsprogramma Informatieveiligheid van Veiligheidsregio's.
 - Tegelijkertijd is er nog veel te doen: het volwassenheidsniveau bereikt nog bij maar weinig organisaties niveau drie, wat minimaal nodig is om een weerbare organisatie te zijn.
- Alle deelnemende organisaties beschikten over [de kernrollen](#) (FG, PO en CISO/(T)ISO).
 - In tegenstelling tot bij SSC's en centrumgemeenten zien we een [duidelijk plafond](#) van rond de 1 fte FG en CISO, ongeacht organisatieomvang.
 - Er is een [algemene groeibehoefte](#), met name op de operationele functies (privacy officer en (T)ISO). VR'en en GGD'en kijken nog weinig naar 'nieuwe' functies, maar zijn vooral nog bezig met de basisfuncties goed in te richten.
- Opvallend is dat [dubbelrollen](#) nog veel voorkomen in deze sector, met name bij VR'en zonder GGD. Vooral de FG-functie moet eraan geloven: deze rol wordt nog té vaak gecombineerd met andere taken, waardoor het de vraag is of deze personen voldoende tijd hebben voor hun adviserende en toezichthoudende taken.
- Organisaties die ICT uitbesteden hadden [een lage IB-formatie](#).
 - Daardoor lopen zij het risico onvoldoende regie te kunnen voeren op hun informatiebeveiliging.

IB&P bij sociaal domein-organisaties

5 Over de deelnemers

De sociaal domein-organisaties (SD's) in dit onderzoek zijn gemeenschappelijke regelingen die namens gemeenten taken uitvoeren op het gebied van het sociaal domein, zoals het uitvoeren van de Participatiewet, de Wet maatschappelijke ondersteuning en de Wet Inburgering. Zij voeren deze taken uit voor meerdere gemeenten. Welke taken zij precies uitvoeren, verschilt per organisatie: sommige voeren alle gemeentelijke taken op Sociaal Domein uit, andere slechts een deel van de gemeentelijke taken, en soms verschilt het takenpakket ook per gemeente.

- In totaal namen er 5 sociaal domein-organisaties deel aan het formatieonderzoek. Vanwege dit kleine aantal is het niet mogelijk om over alle aspecten van het formatieonderzoek te rapporteren, zonder anonimiteit te garanderen. We kiezen er daarom voor om in dit onderzoek stil te staan bij de volgende onderwerpen:
 - Formatie van privacy en informatiebeveiliging;
 - Volwassenheid en ambities van de organisatie op het gebied van privacy en informatiebeveiliging;
 - Dubbelrollen.



5 IB&P bij Sociaal Domein organisaties

Eén van de grote uitdagingen van gemeenten zijn de kosten die vallen onder het sociaal domein, zoals jeugdhulp, inburgering en begeleiding naar werk. Sociaal domein-organisaties zijn vaak taakgericht opgericht, zodat gemeenten hun beperkte middelen gericht kunnen inzetten. Deze organisaties zijn vaak ontstaan door verschillende sociaal domein-afdelingen samen te voegen, of zijn opgericht tijdens de decentralisatie van het sociaal domein in 2015. Het zijn dus relatief jonge organisaties, met een sterke focus op het primair proces. Hierdoor zijn privacy en informatiebeveiliging niet altijd een belangrijk onderwerp geweest. We zien de afgelopen jaren wel een toename van aandacht op IB&P. Dit komt onder andere door de WPG-audit (Wet Politiegegevens) en de NIS2, waar veel sociaal domein-organisaties onder vallen. Ook neemt het bewustzijn bij gemeenten toe, die vervolgens eisen stellen aan deze ketenpartners.

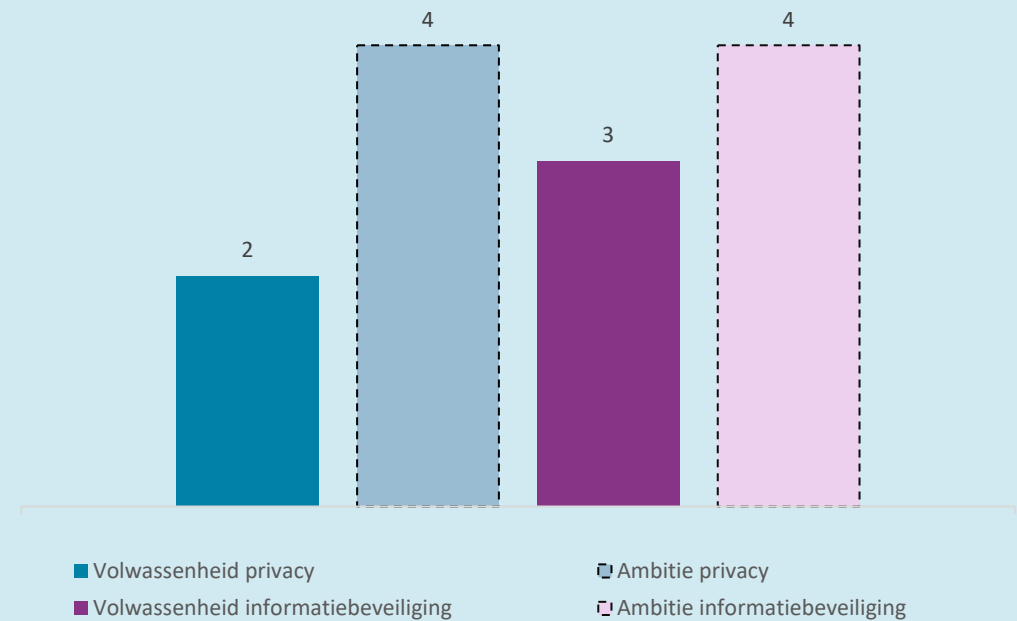
Voorafgaand aan het onderzoek zijn de volgende hypothesen opgesteld over het sociaal domein:

- hoe groter de formatie, hoe volwassener je bent op dat gebied;
- het ambitieniveau ligt hoger dan het volwassenheidsniveau, en parallel daaraan is er een groeibehoefte in formatie over de hele linie;
- de groeibehoefte zit vooral in de operationele rollen (TISO en PO, niet CISO/FG);
- SD's hebben een relatief kleine IB&P-formatie, met name de FG-rol is heel klein;
- 1 fte FG is een 'plafond', ongeacht organisatiegrootte;
- 1 fte CISO is een 'plafond', ongeacht organisatiegrootte;
- combirollen komen veel voor bij sociaal domein-organisaties, inclusief onwenselijke combinaties.

5 Volwassenheid & ambities

- Sociaal domein-organisaties geven aan iets volwassener te zijn op informatiebeveiliging dan op privacygebied. Ze doen dat zelfs uitzonderlijk goed: ze behalen het minimaal gewenste [CMMi-volwassenheidsniveau](#) van 3.
 - Een mogelijke verklaring hiervoor is dat alle deelnemers aangaven dat zij hun ICT uitbesteden; hierdoor hebben ze een deel van de technische beveiliging uitbesteed.
 - Bij privacy is dit niet mogelijk: sociaal domein-organisaties hebben juist heel veel gevoelige persoonsgegevens van kwetsbare inwoners, en hebben dus veel werk te verzetten op privacygebied.
- Alle organisaties rapporteren een hoge ambitie: ze willen in de komende periode naar CMMi-niveau 4 doorgroeien.

Volwassenheid privacy en informatiebeveiliging



Grafiek 15 Gemiddelde volwassenheid privacy en informatiebeveiliging conform het CMMi-model

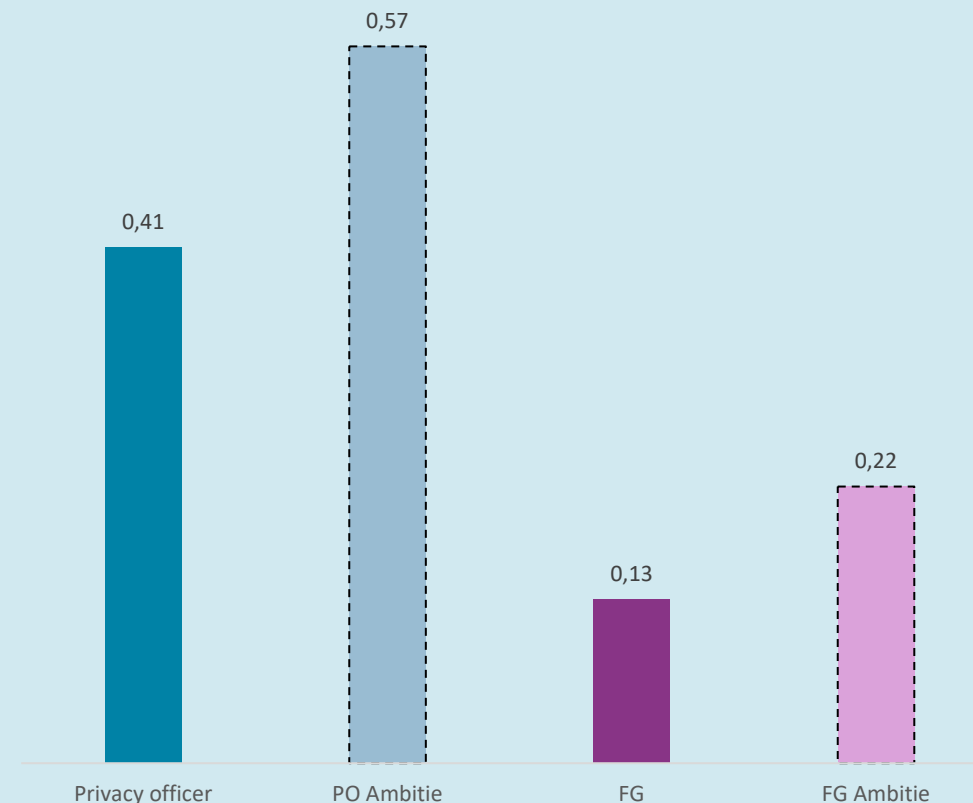
5 Formatie privacy

- In lijn met onze verwachting, was de formatie van privacy laag. Met name de FG-formatie is minimaal: organisaties rapporteerden tussen de 0,06 en 0,33 fte FG in absolute aantallen. Vanwege de grote hoeveelheid inwoners die zij bedienen, leidt dat tot hele lage relatieve aantallen.
 - Desondanks rapporteren de organisaties tevreden te zijn met de FG-formatie: 2 van de 5 organisaties was zelfs volledig tevreden.
 - Er worden niet vaak dubbelrollen vermeld voor de FG-rol, ondanks de lage fte's. Waarschijnlijk wordt de FG vaak ingehuurd of gedeeld met een andere organisatie.

- De privacy officer-rol was zeer variabel: tussen de 0,3 en 1,5 fte in absolute aantallen. Inwoneraantal leek geen bepalende factor in de formatiegrootte van de privacy officer.

- Met name op de privacy officer-rol willen organisaties groeien, met als doel minimaal 0,5 tot maximaal 2 fte.

- Er was geen samenhang tussen privacyvolwassenheid en de grootte van de privacy-organisatie.



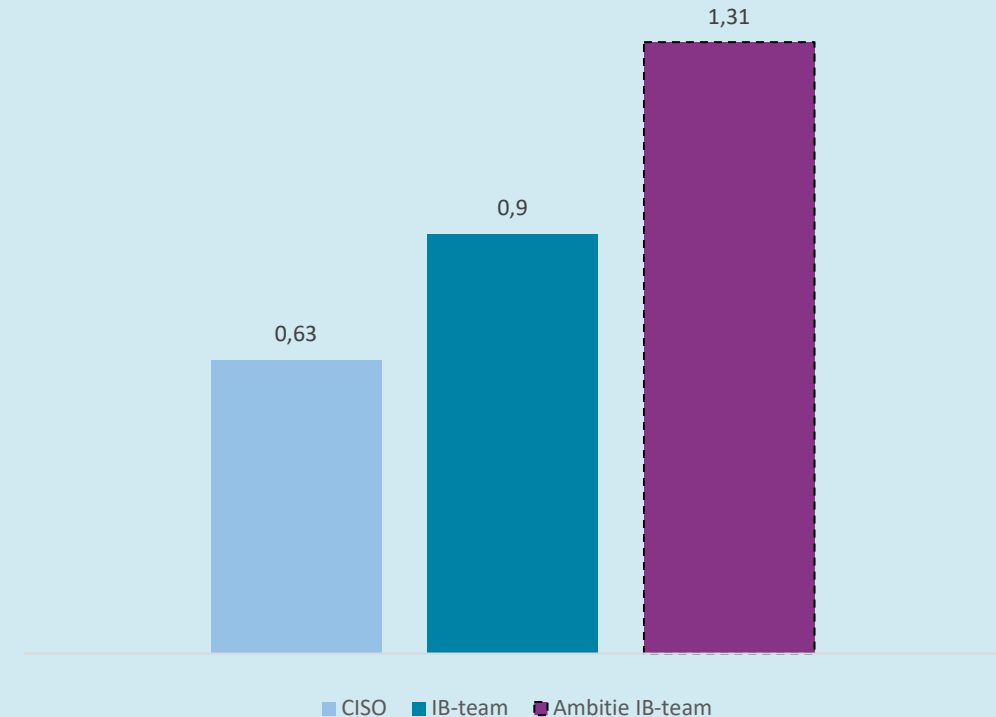
Grafiek 16 Gemiddelde formatie van de functionaris gegevensbescherming en privacy officer per 100.000 inwoners en de ambitie voor komende periode..

5 Formatie Informatiebeveiliging

IB&P BIJ SOCIAAL DOMEIN ORGANISATIES

- Slechts 1 organisatie had een (T)ISO in dienst. Deze is daarom niet weergegeven in de grafiek.
- De CISO-formatie was groter dan verwacht: tussen 0,78 en 2 fte in absolute aantallen. Het 'CISO-plafond' dat we kennen van andere organisaties van maximaal 1 fte, was hier ook weer van toepassing: slechts één organisatie rapporteerde een grotere CISO-formatie.
 - Mogelijk neemt de CISO een deel van de werkzaamheden van de (T)ISO over.
 - Tegelijkertijd is er wel behoefte aan meer [operationele functies](#): sociaal domein-organisaties willen hun team uitbreiden met TISO's en ISO's.
- Daarnaast rapporteerden de sociaal domein-organisaties diverse technische functies als onderdeel van het IB-team, zoals SOC.
- Hoewel de steekproef klein is, is er wel een samenhang te zien tussen IB-formatie en IB-volwassenheid: hoe volwassener de organisatie, hoe groter het IB-team.

Totale IB-formatie per 100.000 inwoners



Grafiek 17 Gemiddelde formatie van de CISO en het IB-team per 100.000 inwoners en de ambitie voor komende periode.

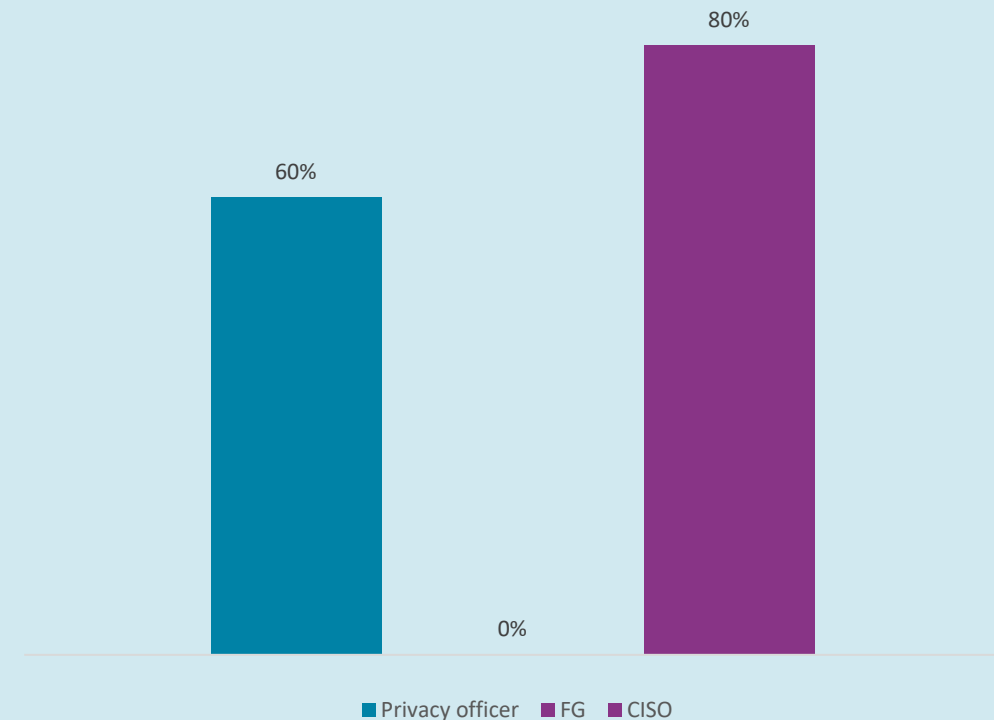
5

IB&P BIJ SOCIAAL DOMEIN ORGANISATIES

Dubbelrollen

- Zoals verwacht komen dubbelrollen heel veel voor bij sociaal domein-organisaties: 3 van de 5 organisaties rapporteerde een dubbelrol voor de privacy officer-functies, en slechts één organisatie had geen dubbelrol voor de CISO.
 - Soms was er sprake van een combinatie van CISO- en PO-functie. Dit kan een risico opleveren voor de organisatie, omdat [strategische/tactische en operationele rollen](#) dan met elkaar verward raken.
 - Ook combineerden zowel CISO's als PO's hun werk met AI-functies.
- Geen enkele FG had een dubbelrol. Een mogelijke verklaring is al eerder genoemd: waarschijnlijk wordt de persoon die deze rol vervuld, ingehuurd of gedeeld met andere organisaties.

Percentage dubbelrollen



Grafiek 18 Percentage van IB&P-functies die tevens een dubbelrol vervuld.

Conclusie: IB&P bij Sociaal Domein-organisaties

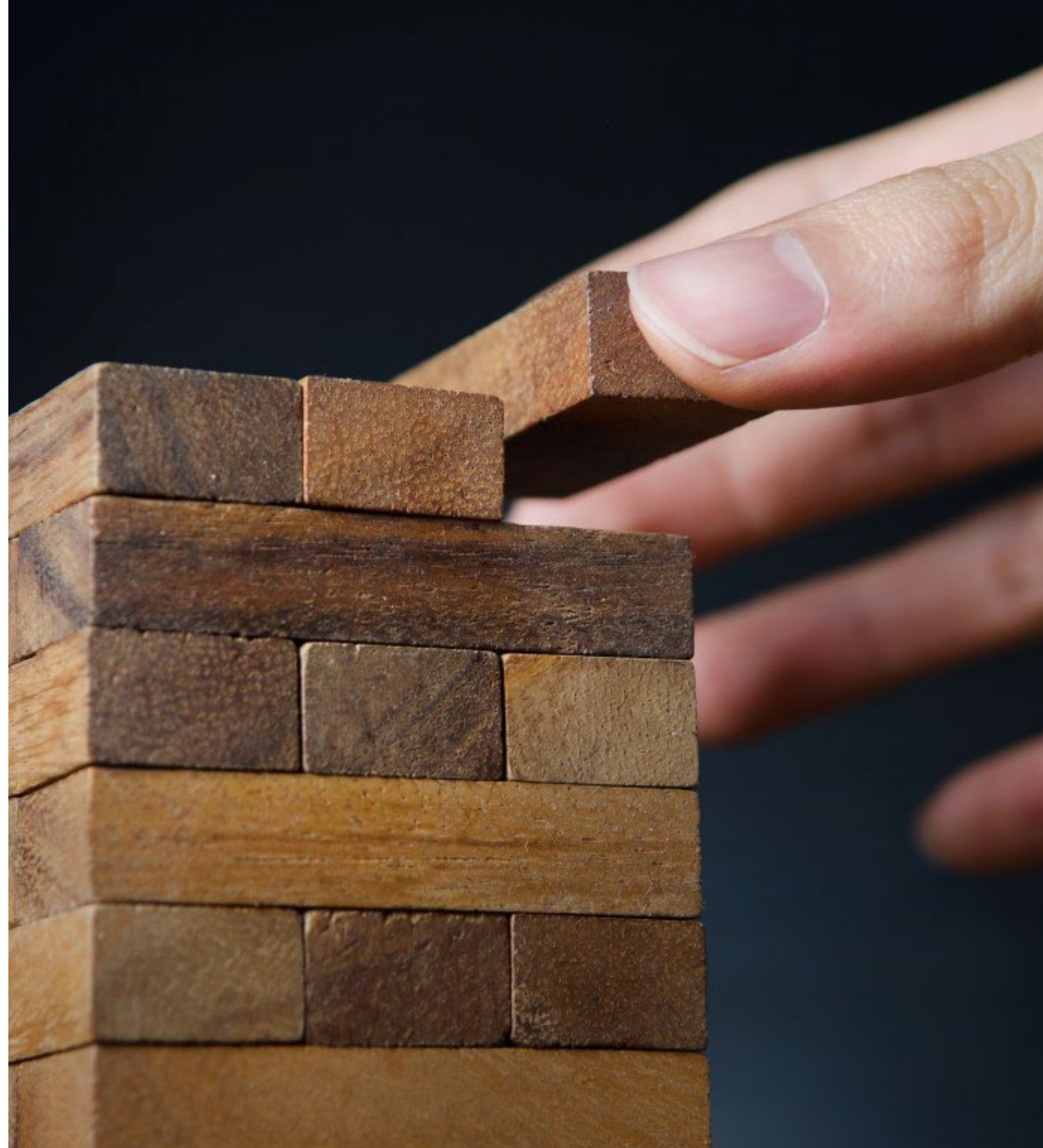
- Sociaal domein-organisaties hebben nog [een kleine IB&P-organisatie](#), ondanks de complexe en privacy-intensieve omgeving waarin zij opereren. Waarschijnlijk speelt hierbij het totale aantal fte van de organisatie een rol: SD-organisaties zijn vaak in absolute zin klein.
 - Desondanks slagen ze er in om op [informatiebeveiligingsgebied](#) behoorlijk volwassen te zijn: het gemiddelde gerapporteerde volwassenheidsniveau is 3. Voor privacy is er een grotere uitdaging: hier zijn organisaties nog niet volwassen, terwijl ze wel gevoelige persoonsgegevens verwerken.
- Er is geen duidelijk verband tussen teamgrootte en organisatievolwassenheid. Het lijkt dus niet zo dat de omvang van het team een allesbepalende factor is voor een meer volwassen organisatie. Mogelijk spelen organisatorische factoren zoals ICT-inrichting en cultuur een grote rol.
 - Desondanks lijken deze organisaties kwetsbaar: IB&P is soms belegd bij slechts één of twee individuen, terwijl deze organisaties grote groepen inwoners bedienen.
 - Het is daarom ook niet vreemd dat de organisaties behoefte hebben om te groeien in hun formatie, waarbij zij vooral op zoek zijn naar mensen die de 'klassieke rollen' zoals privacy officer, TISO en ISO op zich willen nemen.
- Daarnaast is het ook mogelijk dat deze organisaties 'onbewust onbekwaam' zijn: omdat er weinig formatie is, kunnen ze lastig inschatten of ze voldoende weerbaar zijn op privacy- en informatiebeveiligingsgebied.
- Er zijn [veel dubbelrollen](#) bij sociaal domein-organisaties. Door slimme constructies weten zij te voorkomen dat hun FG-rol wordt uitgevoerd door iemand die dit moet combineren met andere interne functies, maar dit geldt niet voor de privacy officer- en CISO-rol. Ook hiervoor geldt dat het organisaties kwetsbaar maakt, bijvoorbeeld bij natuurlijk verloop of uitval.

Conclusie: IB&P bij GR'en

6 De basis staat, maar aandacht blijft nodig

GR'en zoals SSC's, Veiligheidsregio's, GGD'en en sociaal domein-organisaties zetten de afgelopen jaren belangrijke stappen in privacy en informatiebeveiliging: elk van de deelnemende organisaties rapporteerde dat zij een team hadden van informatiebeveiliging- en privacyspecialisten. Tegelijkertijd blijven de aantallen (zowel relatief als absoluut) vaak klein, waardoor deze organisaties kwetsbaar blijven, terwijl ze een belangrijke maatschappelijke opgaven hebben. Ook worstelen ze met dubbelrollen, waarbij ook onwenselijke combinaties voorkomen. Het risico ontstaat dat een slager zijn eigen vlees keurt of waarin strategische/tactische rollen worden gecombineerd met operationele rollen.

Het volwassenheidsniveau van organisaties blijft vaak hangen op *herhaalbaar* (niveau 2), wat aangeeft dat zij onvoldoende weerbaar zijn. Wel ambiëren alle organisaties om in privacy en informatiebeveiliging te groeien. De vraag is in hoeverre deze ambities haalbaar zijn als extra uitbreiding van het team uitblijft. Informatiebeveiliging en privacy moeten nooit beperkt zijn tot een team van specialisten, maar deze specialisten zijn wel essentieel voor het creëren van een sterke IB&P-organisatie.



Onderzoeksmethodiek

Onderzoeksmethodiek

Dataverzameling

Dit onderzoek maakt gebruik van de online enquête *Formatieonderzoek 2025: privacy en informatiebeveiliging in de lokale overheid*, die breed is verspreid binnen de overheidssector. Om een representatief en betrouwbaar beeld te krijgen, werden er proactief personen uit het netwerk van M&I/Partners benaderd. Verder werd de vragenlijst verspreid via LinkedIn en sectorspecifieke netwerken, zoals het VNG forum en vaste overlegstructuren binnen de sector. In het onderzoek vroegen we:

- **de huidige formatie op privacy en informatiebeveiliging.**
 - om de formatie van het privacyteam in beeld te krijgen, werd gevraagd naar de formatie van de privacy officer en de FG.
 - Voor informatiebeveiliging is om formatiecijfers van de CISO, (T)ISO en het IB-team gevraagd. In het IB-team kunnen ook personen zitten die niet onder de functie CISO of (T)ISO vallen. Via een vrij vragenveld konden respondenten aangeven welke eventuele additionele functies aanwezig zijn.
- Dit jaar werd gevraagd of er sprake was van **dubbelrollen** binnen de privacy- en IB-organisatie, door te vragen of de personen die de rol van FG/PO/CISO/(T)ISO bekleden, ook een andere rol of functie bekleedden.

- De antwoorden zijn achteraf gecorrigeerd: als organisaties aangaven dat er sprake was van een dubbelrol vanwege inhuur (ofwel, deze persoon bekleedde een andere rol bij een andere organisatie), is dit gewijzigd naar 'geen dubbelrol'.
- De **gewenste formatie** op privacy en informatiebeveiliging;
 - Het huidige volwassenheidsniveau op privacy en informatiebeveiliging, op basis van [het CMMi](#);
 - Het geambieerde volwassenheidsniveau op privacy en informatiebeveiliging, op basis van [het CMMi](#).

Onderzoeksmethodiek

Respondenten

De enquête is voornamelijk ingevuld door specialisten op het gebied van privacy en security, zoals Functionarissen Gegevensbescherming (FG's), Chief Information Security Officers (CISO's) en Privacy Officers (PO's), of hun leidinggevenden. Dit waarborgt dat de antwoorden afkomstig zijn van professionals met directe kennis van de formatie(behoeft) en het volwassenheidsniveau van hun organisatie.

In totaal vulden 68 verschillende respondenten van 66 verschillende lokale overheidsorganisaties de vragenlijst in. Er deden **31 GR'en** mee. Om dubbele antwoorden te voorkomen, vroegen we de naam van de organisatie uit. Bij dubbele antwoorden werd het gemiddelde antwoord berekend.

Analyse

Om de cijfers vergelijkbaar te maken, zijn de fte's berekend per 100.000 inwoners. 1 fte komt overeen met een werkweek van 36 uur.

Categorie	Aantal respondenten
SSC's en centrumgemeenten	13
Veiligheidsregio's en GGD'en	13
Sociaal domein-organisaties	5

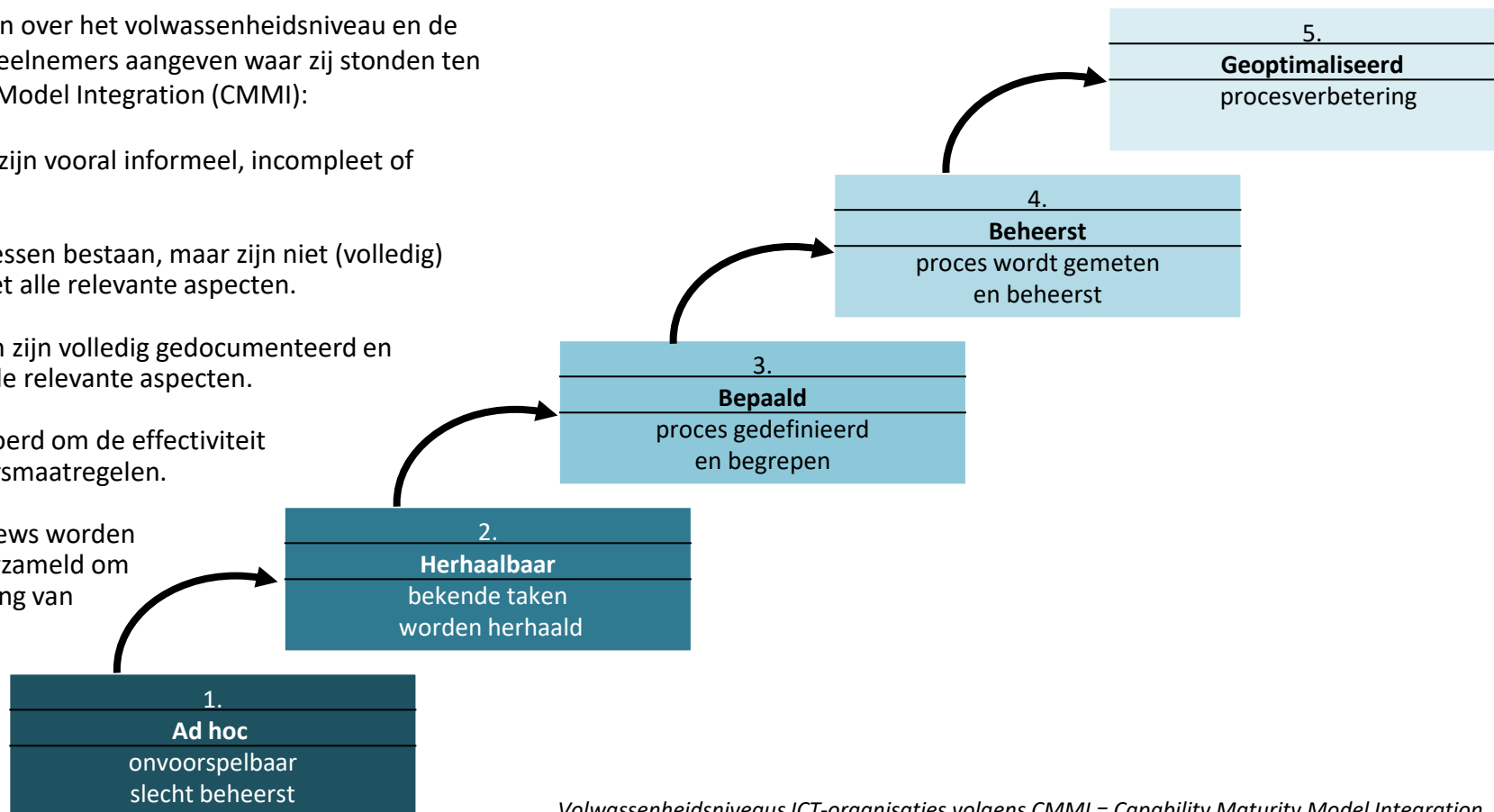


Bijlagen

8 Het CMMi

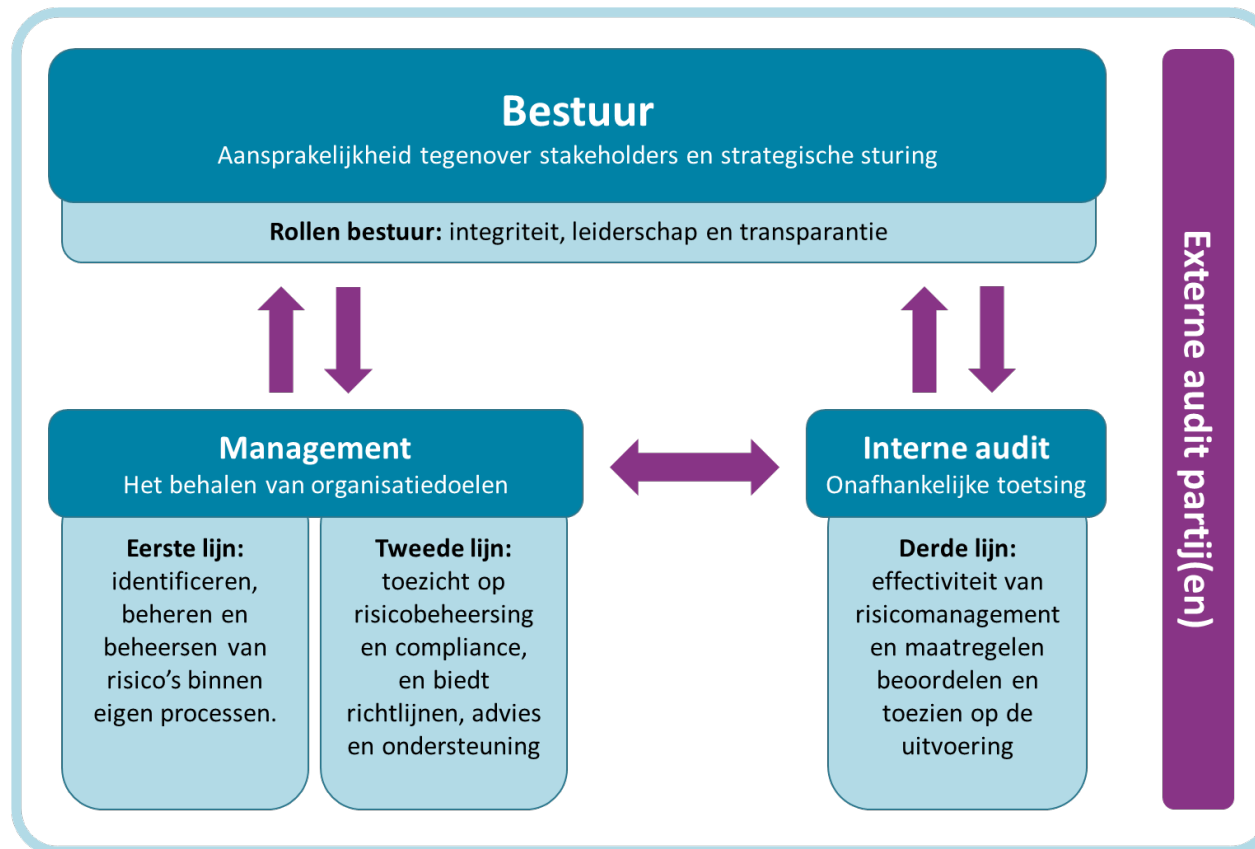
Voor het beantwoorden van de vragen over het volwassenheidsniveau en de ambitie van de organisatie, konden deelnemers aangeven waar zij stonden ten opzichte van het Capability Maturity Model Integration (CMMI):

1. **Ad hoc:** procedures of processen zijn vooral informeel, incompleet of worden inconsistent toegepast.
2. **Herhaalbaar:** procedures of processen bestaan, maar zijn niet (volledig) gedocumenteerd en omvatten niet alle relevante aspecten.
3. **Bepaald:** procedures of processen zijn volledig gedocumenteerd en geïmplementeerd en omvatten alle relevante aspecten.
4. **Beheerst:** reviews worden uitgevoerd om de effectiviteit te meten van de getroffen beheersmaatregelen.
5. **Geoptimaliseerd:** periodieke reviews worden uitgevoerd en feedback wordt verzameld om te zorgen voor continue verbetering van procedures of processen.



Volwassenheidsniveaus ICT-organisaties volgens CMMI = Capability Maturity Model Integration

8 Three lines model



Legenda ↑ Verantwoording, rapporteren ↓ Delegatie, sturing, middelen, overzicht ↔ Afstemming, communicatie, coördinatie, samenwerking

8 Toelichting ICT-inrichting

In ons onderzoek konden organisaties kiezen uit vijf mogelijke opties voor ICT-inrichting:

- de organisatie heeft de ICT zelf in huis én levert ICT-diensten aan andere partijen;
- de organisatie heeft zelf de ICT in huis;
- de organisatie heeft deels de ICT in huis, en deels uitbesteed;
- de organisatie heeft haar ICT uitbesteed aan een andere overheidsorganisatie zoals een centrumgemeente of een gemeenschappelijke regeling;
- de gemeente heeft haar ICT uitbesteed aan een gespecialiseerde ICT-leverancier.

Om herleidbaarheid te verminderen, zijn deze antwoorden in het onderzoek geëxtraheerd:

Oorspronkelijke antwoord	Categorie
De organisatie heeft de ICT zelf in huis én levert ICT-diensten aan andere partijen	ICT in huis
De organisatie heeft zelf de ICT in huis	
De organisatie heeft deels ICT in huis, en deels uitbesteed	Combinatie
De organisatie heeft haar ICT uitbesteed aan een andere overheidsorganisatie	Uitbesteed
De organisatie heeft haar ICT uitbesteed aan een gespecialiseerde ICT-leverancier	

Meer weten?
www.mxi.nl



Marit Wensink
Informatiebeveiliging en privacy

06 13 39 07 47
marit.wensink@mxi.nl



Pauline Hogendoorn
Benchmark

06 82 05 83 34
pauline.hogendoorn@mxi.nl