2024

FORMATIEONDERZOEK INFORMATIEBEVEILIGING BIJ GEMEENTEN

Sparrenheuvel 32, 3708 JE Zeist | (030) 2 270 500 | info@mxi.nl | www.mxi.nl

Marit Wensink & Matthijs Verzijl

Hoe ziet het privacy- en informatiebeveiligingsteam van lokale overheidsorganisaties eruit? Wat is een passende omvang voor ons IB-team ten opzichte van onze ambities? Hoe verhoudt onze formatie zich ten opzichte van andere overheidsorganisaties?

Regelmatig ontvangen we bij M&I/Partners dit soort vragen van klanten. In 2022 deden we daarom een uitvraag naar de formatie van de Functionaris Gegevensbescherming (FG) en Privacy Officer (PO) bij overheidsorganisaties. Afgelopen jaar deden we deze uitvraag opnieuw, ditmaal uitgebreid met vragen over de informatiebeveiligingsformatie. In een eerdere blog deelden we de resultaten over de formatie en ambities voor privacy. In dit artikel delen we de resultaten van het formatieonderzoek van 2024 voor informatiebeveiliging.

ONTWIKKELINGEN IN INFORMATIEBEVEILIGING

Voordat we de cijfers induiken, kijken we naar de ontwikkelingen in de afgelopen tijd en de komende jaren. De afgelopen jaren groeide de aandacht voor informatiebeveiliging in gemeenten sterk, en we verwachten dat deze aandacht de komende jaren alleen nog maar verder toeneemt. In 2024 is de Baseline Informatiebeveiliging Overheid herzien en herschreven tot de BIO2.0 (nog in concept). In de BIO2.0 wordt het aanstellen van een CISO als eis opgenomen[1]. Daarnaast ging in oktober 2024 de NIS2 in (naar verwachting is de Nederlandse vertaling, de Cyberbeveiligingswet, in het voorjaar van 2026 van toepassing). Ook stelde de Vereniging van Nederlandse Gemeenten (VNG) in haar uitvoeringsanalyse dat de AI Act impact gaat hebben op de werkzaamheden van hun IT- en informatiebeveiligingsteam[2].

Tegelijkertijd worstelen gemeenten met het complexe IT-landschap, dat steeds complexer wordt. Dit heeft te maken met drie factoren die in elkaars verlengde liggen:

1. Steeds meer applicaties zijn niet meer in eigen beheer (on premise), maar staan ‘in de cloud’ (SaaS, Software-as-a-Service), zoals blijkt uit onze ICT Benchmark gemeenten. Hoe meer ICT zich in de cloud bevindt, hoe lastiger het voor gemeenten wordt om goed controle en overzicht op alles te houden.

[1] Zie overheidsmaatregel 5.02.02 van de Concept Baseline Informatiebeveiliging Overheid 2, versie 1.1 van 14 april 2025.

[2] Schram, J., Zutphen, F. van, & Beek, A. van (2024). *Uitvoeringsnalayse Digital Decade AI-verordening*.

2 Bij verSaaSing zien we ook dat harde IT-kennis over de systemen steeds meer bij de leverancier komt te liggen, en niet langer bij de organisatie zelf.
3 Tegelijkertijd blijven vaak oude applicaties nog bestaan, die soms nog on premise draaien. Er is vaak nog automatiseringspersoneel nodig die deze applicaties onderhouden.

Gemeenten, zowel groot als klein, besluiten regelmatig om een groot deel of hun gehele ICT te beleggen bij Shared Service Centra (SSC's), in de hoop dat zij hierdoor sterker staan in het complexe IT-landschap, tegen minder kosten. Maar bij uitbesteding van de ICT is er geen sprake van volledige uitbesteding van informatiebeveiliging: gemeenten dienen zelf áltijd regie te houden op hun ICT-dienstverlening en zijn verantwoordelijk voor een adequate beveiliging daarvan. Zij stellen de kaders en leggen eisen op aan hun dienstverleners. Ook bij uitbesteding is dus IB-formatie noodzakelijk.

HYPOTHESEN

Met het oog op bovenstaande ontwikkelingen verwachtten we dat uit ons formatieonderzoek zal blijken dat er sprake is van een zekere 'ondergrens' in IB-formatie (geen enkele gemeente zal géén informatiebeveiligingspersoneel in dienst hebben), en dat er behoefte is aan groei. We verwachtten ook dat SSC's een grotere IB-formatie hebben, en dat zij een hogere IB-volwassenheid hebben vanwege hun gespecialiseerde dienstverlening.

Kader: onderzoeksmethodiek

Dit formatieonderzoek is gebaseerd op een online enquête, die breed is verspreid binnen de overheidssector. Om een representatief en betrouwbaar beeld te krijgen, benaderden we proactief personen uit ons eigen netwerk en deelden we de enquête via LinkedIn. In het onderzoek vroegen we naar de huidige én gewenste formatie op privacy en security en naar het huidige én gewenste volwassenheidsniveau. We vroegen voor de informatiebeveiligingsformatiecijfers om formatiecijfers van de CISO, (T)ISO en het IB-team. In het IB-team kunnen ook personen zitten die niet onder de functie CISO of (T)ISO vallen.

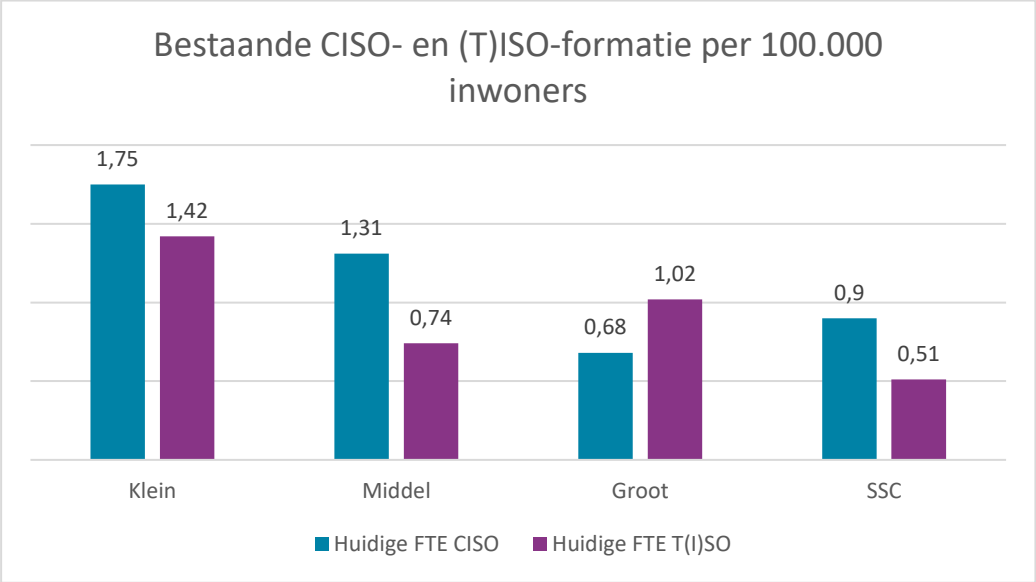
De enquête is voornamelijk ingevuld door specialisten op het gebied van privacy en security, zoals Functionarissen Gegevensbescherming (FG's), Chief Information Security Officers (CISO's) en Privacy Officers (PO's), of hun leidinggevenden. Dit waarborgt dat de antwoorden afkomstig zijn van professionals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

In totaal vulden 56 verschillende respondenten van 46 verschillende lokale overheidsorganisaties de vragenlijst in. Er deden 33 gemeenten en 7 Shared Service Centers mee. Om dubbele antwoorden te voorkomen, vroegen we de naam van de organisatie uit. Bij dubbele antwoorden werd het gemiddelde antwoord berekend.
Overige organisaties waren Sociale Diensten, veiligheidsregio's en GGD'en. Vanwege de beperkte steekproef van deze organisaties zijn de cijfers niet meegenomen in het onderzoek.

Gemeenten worden ingedeeld in:
- Grote gemeente: 100.000+ inwoners;
- Middelgrote gemeente: 50.000-100.000 inwoners;
- Kleine gemeente: minder dan 50.000 inwoners.

Om de cijfers vergelijkbaar te maken, worden fte's omgerekend naar *per 100.000 inwoners*.

HUIDIGE INFORMATIEBEVEILIGING-FORMATIE



In het onderzoek vroegen we wat de huidige formatie is van het totale IB-team, de CISO en de (Technical) Information Security Officers ((T)ISO's). Relatief gezien hebben kleine gemeenten de grootste formatie met een CISO-formatie van 1,75 fte per 100.000 inwoners. We zien dat er, zoals verwacht, sprake is van een soort 'onder- en bovengrens' als het gaat om formatiecijfers van het IB-team.

Type organisatie	Aantal fte IB-formatie in absolute aantallen	Aantal fte CISO in absolute aantallen	Aantal fte (T)ISO in absolute aantallen
Kleine gemeente	1,14 fte	0,68 fte	0,51 fte
Middelgrote gemeente	1,77 fte	0,94 fte	0,53 fte
Grote gemeente	5,58 fte	1,08 fte	1,8 fte
SSC	3,04 fte	1,21 fte	1,13 fte

Tabel 1: fte's IB-formatie in absolute aantallen

- Gemeenten rapporteren een minimale absolute CISO-formatie van 0,50 fte. Elke gemeente en elk SSC, groot of klein, heeft dus minimaal een half fte CISO in dienst (of huurt deze in). We zien in de praktijk bij kleine gemeenten dat de CISO-formatie gedeeld wordt: één persoon is fulltime CISO, in dienst bij twee verschillende (kleine) gemeenten. Zo zorgen kleine gemeenten dat zij voldoende kennis en kunde in huis hebben zonder dat zij de volledige lasten hoeven te dragen.

- De (T)ISO-formatie bij kleine en middelgrote gemeenten is ook ongeveer een 0,51 – 0,53 fte. Mogelijk wordt deze rol ook vaker gedeeld met andere gemeenten. Een andere verklaring is dat de (T)ISO twee rollen binnen de gemeente combineert. Bij de voor- en nadelen van combinatierollen staan we in de volgende paragraaf stil.

- Gemeenten en SSC's rapporteren een CISO-formatie van gemiddeld 1,3 fte per 100.000-inwoners. In absolute aantallen is te zien dat de CISO-formatie van gemeenten tussen de 0,68 en 1,08 fte ligt. Gemeenten hebben dus maximaal 1,0 fte CISO in dienst (en zeer waarschijnlijk ook één persoon). Deze trend zagen we in ons onderzoek ook al bij de cijfers van de privacyformatie: gemeenten hebben maximaal één FG in dienst, en breiden deze formatie niet verder uit.

- Opvallende uitzondering hierin zijn de SSC's, die een hogere CISO-formatie rapporteren (1,21 fte). Zij hebben vaak meer dan één CISO in dienst. Hiervoor zijn twee mogelijke verklaringen:
  - Doordat SSC's meerdere gemeenten bedienen, hebben zij een complexer IT-landschap, dat vraagt om meerdere CISO's om goed grip te houden op de informatiebeveiliging.
  - Soms lenen SSC's CISO's uit aan gemeenten aan wie zij dienstverlening leveren. Dat betekent dat een CISO formeel in dienst is bij een SSC, maar werkzaamheden verricht voor de klantgemeenten. Het verdelen van deze lasten over meer dan één persoon is niet vreemd, zeker niet als de SSC een groot aantal klantgemeenten bediend.

- Opvallend en onverwacht is dat SSC's een relatief lage (T)ISO-formatie hebben. Wij verwachtten dat deze groter zou zijn, omdat zij meer specialistische technische kennis nodig hebben gezien hun type dienstverlening. Een mogelijke verklaring hiervoor is dat hun CISO een deel van deze technische kennis brengt. CISO's in dienst bij gemeenten zijn niet altijd enorm technisch, maar brengen ook belangrijke organisatorische en procesmatige kennis in. SSC's geven waarschijnlijk voorkeur aan een technisch sterkere CISO, waardoor er minder specialistische kennis op de (T)ISO-rol nodig is.

Combi-rollen

Naast dat gemeenten CISO's en (T)ISO's delen met andere gemeenten, kunnen zij er ook voor kiezen om deze functies intern te combineren met andere rollen. De afgelopen jaren zagen we verschillende combinaties voorbijkomen, waarvan de combinatie CISO/FG en ISO/PO het meest voorkomen. Hieronder gaan we kort in op deze rollen:

ISO/PO

Zeker in kleine gemeenten komen we regelmatig de combinatierol van information security officer/privacy officer tegen, ook wel afgekort tot PSO. Deze gemeenten worstelen met beperkte middelen en zien in het combineren van deze rol een oplossing: ze kunnen één fulltime vacature openstellen en daar één persoon voor inzetten. Het verdelen van de rollen over meerdere personen is lastiger, omdat het werven van personen die 18 uur per week willen werken moeilijker is dan het werven van personen die 36 uur werken. Bovendien zou 0,5 PO en 0,5 (T)ISO vragen om afstemming tussen beide personen, wat weer voor snijverlies zorgt.

Maar er zitten ook risico's verbonden aan deze combinatie. De twee grootsten: gebrek aan kennis en het dienen van verschillende doelen.

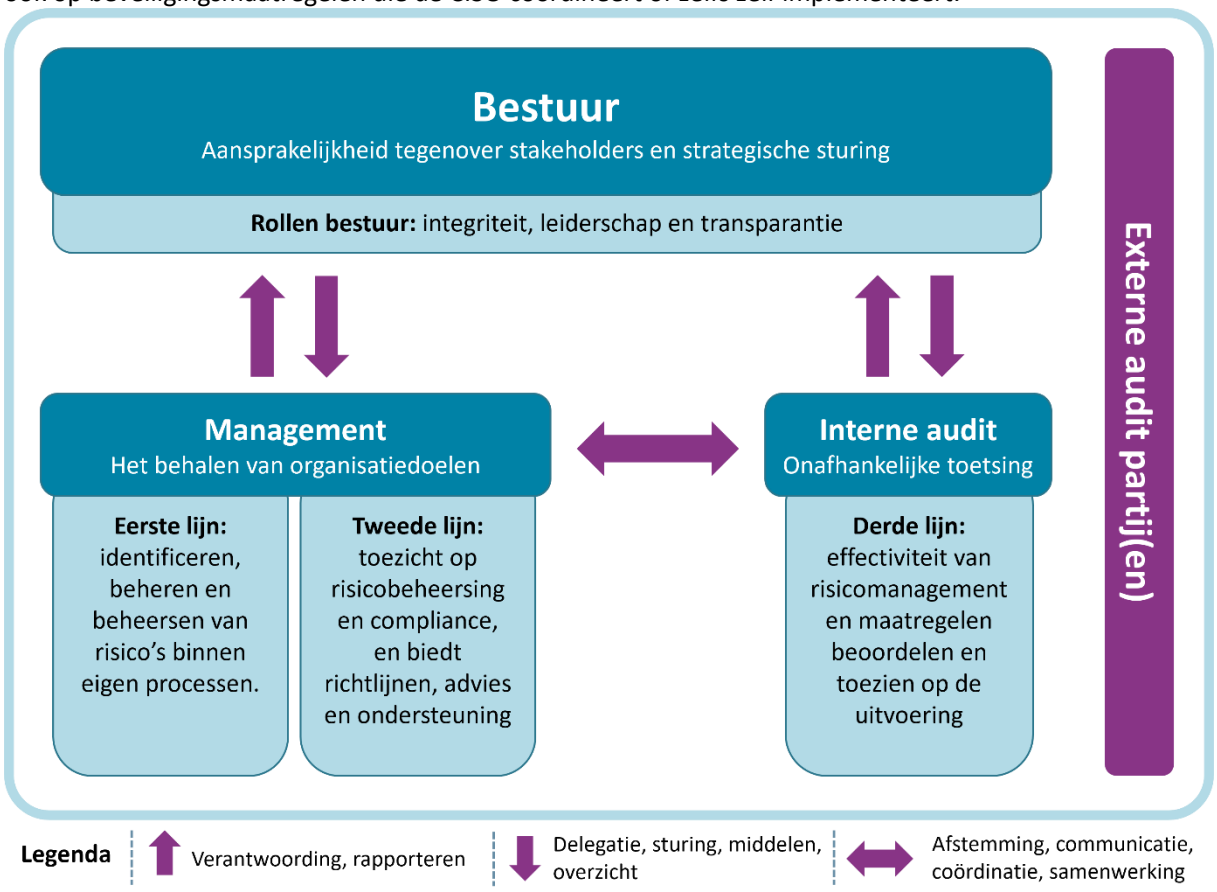
- Het privacy- en security-vakgebied zijn beide gespecialiseerde vakgebieden die vragen om veel inhoudelijke kennis. Een Privacy Officer moet veel weten van de AVG en gelieerde wet- en regelgeving, maar ook van informatiemanagement in de brede zin van het woord. Een Security Officer heeft vaak meer technische kennis en staat vaak wat verder van het primaire proces af dan de privacy officer (niet geheel verrassend wordt de Security Officer vaak gepositioneerd in het IT-team). Het combineren van de rollen betekent ook het combineren van kennis, en de vraag is of deze kennis voldoende in één persoon te vinden is.

- Daarnaast hebben privacy en security twee essentieel verschillende doelen en focus. Privacy gaat om het beschermen van de persoonsgegevens van de betrokkene: de persoon, over wie er gegevens verwerkt worden, staat centraal. Security gaat over het beschermen van de bedrijfsbelangen. Deze doelen kunnen soms haaks op elkaar staan. Dat betekent dat de PSO moet kiezen welke belangen hij richting het management vertegenwoordigd: die van de organisatie of die van de betrokkene.

Gemeentes die extern een vacature openstellen voor een PSO, merken dat het moeilijk is om hier geschikt personeel op te werven, mede doordat er een breed palet aan kennis vereist is. Intern lukt het soms wel om de rol te vullen: iemand die al in dienst is als privacy officer neemt geleidelijk meer security officer taken op zich, of vice versa. Hoewel dit een oplossing kan lijken voor het personeels- en middelentekort, is het dus de vraag of dit wenselijk is.

CISO/FG

De combinatie van de CISO-rol met die van Functionaris Gegevensbescherming komt minder vaak voor dan de combinatie van ISO en PO. Dit heeft te maken met de positionering van de CISO: soms is deze, net als de FG, op de derde lijn van het *three lines of defense*-model gepositioneerd (toezichthoudend/adviserend), maar regelmatig is deze meer ondersteunend aan de uitvoering en bevindt zich dan in de tweede lijn. Een CISO die zich in de tweede lijn bevindt, kan de rol onmogelijk combineren met de derdelijns functie van toezichthouder. Er is namelijk heel snel sprake van een "slager die zijn eigen vlees keurt": de FG houdt toezicht op de beveiliging van persoonsgegevens en daarmee dus ook op beveiligingsmaatregelen die de CISO coördineert of zelfs zelf implementeert.



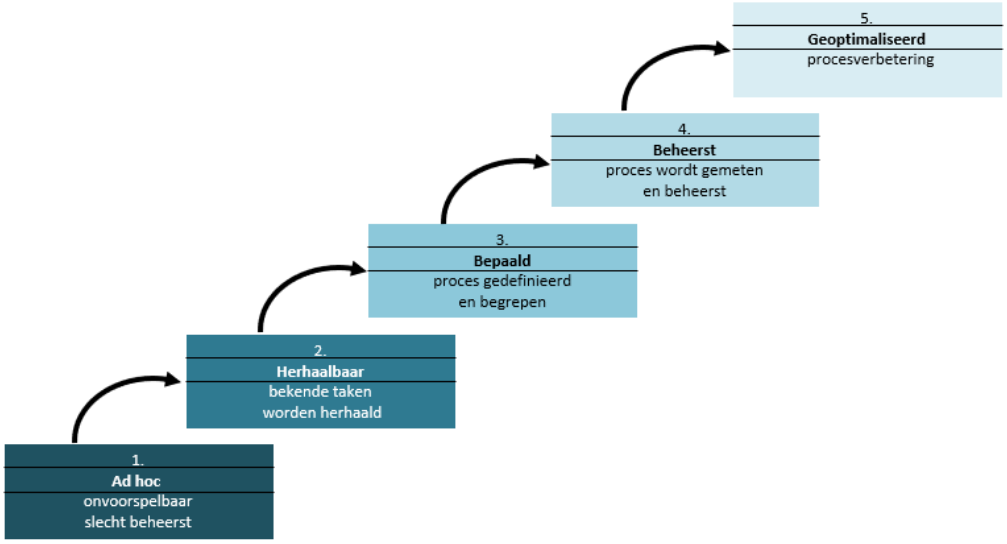
Figuur 1: Three Lines of Defense Model - Riskworld

IB-VOLWASSENHEID

In het onderzoek vroegen we deelnemers naar hun huidige en gewenst volwassenheidsniveau op informatiebeveiligingsgebied. Daarbij hanteerden we de volgende definities en niveaus (volgens 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 continu verbetering van procedures of processen.



Figuur 2: Volwassenheidsniveau 's ICT organisatie volgens Capability Maturity Model Integration (CMMI)

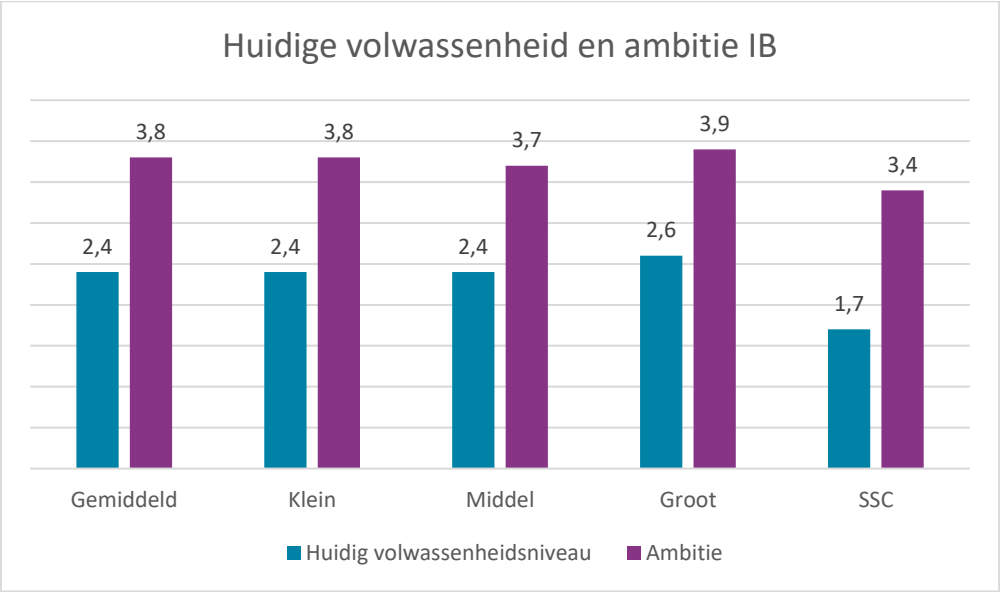
Gemiddeld rapporteerden alle gemeenten SSC's een volwassenheidsniveau tussen 'herhaalbaar' en 'gedefinieerd' (2,4). Er zijn slechts hele kleine verschillen tussen gemeenten, waarbij grote gemeenten gemiddeld een iets hoger volwassenheidsniveau hebben bereikt (2,6) dan kleine en middelgrote gemeenten. Een mogelijke verklaring hiervoor is dat zij meer middelen hebben, waardoor ze sneller kunnen groeien in volwassenheid; maar ze worden weer direct afgeremd door een complexer IT-landschap. Hierdoor wordt de groei enerzijds versneld en anderzijds vertraagd, resulterend in een vergelijkbaar volwassenheidsniveau.

Een opvallende achterblijver zijn de SSC's, die een gemiddeld volwassenheidsniveau rapporteren van 1,7. Dit staat haaks op de verwachtingen die wij regelmatig horen van gemeenten: dat het uitbesteden van de IT naar een SSC (inclusief een groot deel van de technische informatiebeveiligingsvereisten) resulteert in een hoger beveiligings- en volwassenheidsniveau. Wij zien twee factoren die zorgen dat SSC's achterblijven in volwassenheid:

- De meeste SSC's hebben te maken met een nog complexere infrastructuur dan een gemiddelde gemeente. Zij leveren dienstverlening aan gemeenten met elk hun eigen IT-infrastructuur en applicatielandschap.

- In de afgelopen tijd kozen gemeenten er regelmatig voor om hun IT-afdelingen gezamenlijk onder te brengen onder één gemeenschappelijke regeling en een (vaak nieuw) SSC. Dit gaat vaak gepaard met een bezuinigingsslag, met het idee: "als we de IT samendoen, kunnen we dit met minder middelen". Dit zien we ook terug in de cijfers: SSC's hebben relatief gezien een veel lagere formatie dan de gemeenten die zij bedienen (respectievelijk 3,04 fte IB-formatie per 100.000 inwoners tegenover 5,57 fte per 100.000 inwoners bij grote gemeenten). Zo'n reorganisatie vraagt echter om strakke begeleiding en sturing en een goede organisatie, die ontbreekt. Zo krijgen SSC's te maken met een

'valse start' die zij moeilijk inlopen. Gemeenten hopen met het uitbesteden van formatie een kwaliteitsslag te slaan, maar dit vraagt om goede investeringen.



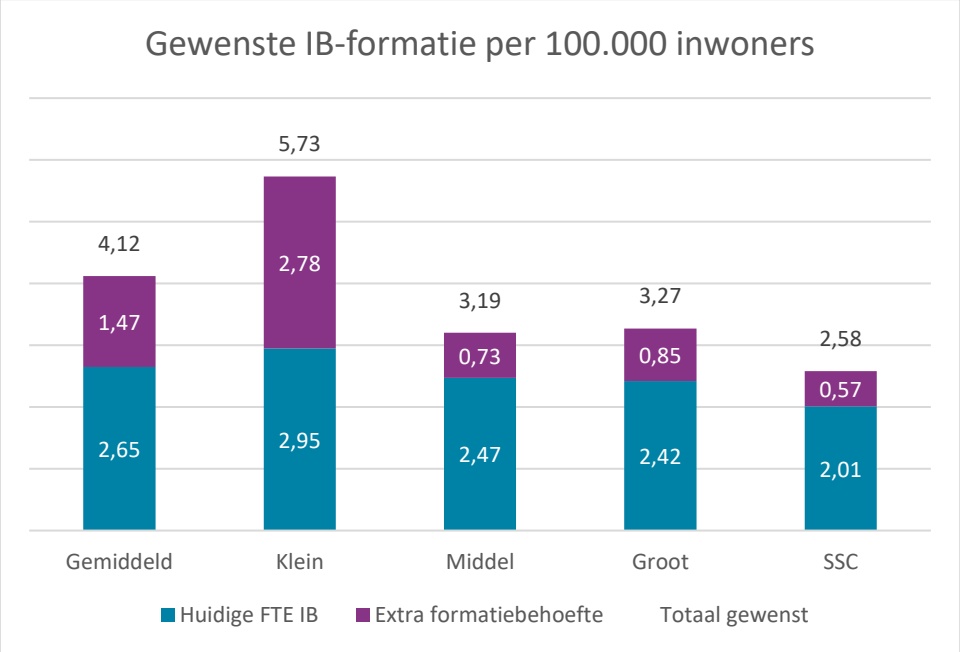
Alle gemeenten en SSC's gaven aan dat zij streven naar een volwassenheidsniveau tussen 3 en 4 (gemiddeld 3,76). Dit sluit aan bij recente ontwikkelingen op het gebied van wet- en regelgeving en bij de uitdagingen die gepaard gaan met de toename van het gebruik van AI.

SAMENHANG TUSSEN VOLWASSENHEID EN FORMATIEBEHOEFTE

De wens van overheidsorganisaties om te groeien in IB-volwassenheid vertaalt zich rechtsreeks in een groeibehoefte. In onze uitvraag focusten we ons op de totale IB-formatie (dus niet gespecificeerd in CISO- of (T)ISO-groei), omdat we weten dat IB-formatie kan bestaan uit extra rollen naast de CISO en de (T)ISO, zoals een cybersecurityspecialist.

Alle gemeenten en SSC's geven aan dat zij meer fte's IB in hun formatie wensen Waar we bij de cijfers van de privacyformatie een soort 'plafond' aantroffen (waarbij organisaties met een grote formatie minder groeibehoefte hadden, onafhankelijk van volwassenheidsniveau en -ambitie), lijkt daar bij IB-formatie geen sprake van.

Opvallend is dat bij kleine gemeenten de (relatief) grootste groeibehoefte is. We hebben geen formatiecijfers uit eerdere jaren beschikbaar, maar we vermoeden dat kleine gemeenten bezig zijn met een 'inhaalslag': eerder leunden zij sterk op hun IT-leverancier of centrumgemeente in de verwachting dat die hen konden helpen met informatiebeveiligingsvolwassenheid. Inmiddels kwamen ze tot de realisatie dat informatiebeveiliging niet volledig buiten de eigen organisatie kan plaatsvinden. De afgelopen jaren zetten zij de eerste stappen, maar waarschijnlijk zien gemeenten toename in formatie als enige mogelijkheid om verder te groeien in volwassenheid.



CONCLUSIE: REGIE OP IB

Informatiebeveiliging is een structureel en onmisbaar onderdeel van de gemeentelijke organisatie, blijkt uit de resultaten van ons onderzoek. Ondanks verschillen in inwoneraantal, is er bij álle typen organisaties een duidelijke ambitie om te groeien in IB-volwassenheid én formatie. Vooral kleine gemeenten tonen een sterke groeibehoefte, mogelijk als gevolg van een inhaalslag. Hoewel we niet expliciet uitvroegen of de deelnemende gemeenten hun IT in huis of bij een IT-leverancier of centrumgemeente belegden, weten we uit ervaring dat kleine en middelgrote gemeenten hun IT vaker uitbesteden. Uit de ICT Benchmark Gemeenten 2024 blijkt dat het IT-landschap complexer wordt, met een toename van SaaS-oplossingen en hybride infrastructuren.

De ontwikkelingen op AI-gebied zorgen voor mogelijkheden, maar ook voor nieuwe dreigingen. Daarnaast neemt de hoeveelheid wet- en regelgeving die impact heeft op informatiebeveiliging toe. Dit vraagt om meer regie, meer kennis en dus ook meer formatie op informatiebeveiliging. Kortom, informatiebeveiliging is essentieel in overheidsorganisaties, óók als zij IT uitbesteden.

Marit Wensink
- marit.wensink@mxi.nl
- 06 13 39 07 47

Matthijs Verzijl
- matthijs.verzijl@mxi.nl
- 06 12 15 31 19