VNG Realisatie

Handreiking carve-out Suwinet

Toetsingsmethodiek ENSIA-verantwoording 2023

VNG Realisatie

Nassaulaan 12
2514 JS Den Haag

Juli 2023

Inhoud

1. Inleiding

1.1. [1]Carve-out voor Suwinet

In 2020 werd de carve-out methodiek geïntroduceerd voor Gezamenlijke Elektronische Voorzieningen SUWI (GeVS/Suwinet). Deze werkwijze bestaat al voor DigiD en wordt vanaf 2020 ook toegepast worden voor gemeenten die diensten hebben uitbesteed én waar het raadplegen van Suwinet onderdeel uitmaakt van het bedrijfsproces bij de serviceorganisatie/leverancier én waarbij de verantwoording Suwinet aan de gemeente wordt vormgegeven met een Third Party Mededeling (TPM).

De **carve-out** methodiek gaat uit van een klant-leverancier relatie en heeft betrekking op verantwoordelijkheden van de betrokken auditors. Bij een carve-out methodiek kan en wordt bij voorkeur gebruik gemaakt van een TPM. Een IT-auditor (met kwalificatie Register EDP-Auditor (RE) voert het onderzoek uit en beoordeelt of de leverancier voldoet aan de eisen van de verantwoordingsrichtlijn, vastgesteld door de SUWI-partijen. De TPM wordt 'assertion based' opgeleverd aan de gemeente. Deze fungeert als opdrachtgever en is de partij die verantwoording over het geheel van het gebruik van Suwinet aflegt.

Bij de carve-out methodiek:

- Voert de IT-auditor van de gemeente geen (separaat) onderzoek uit naar de processen begrepen in de ontvangen TPM('s) van serviceorganisatie(s) en de oordelen daarbij.
- Neemt de auditor van de gemeente (dan ook) geen verantwoordelijkheid voor de oordelen die zijn opgenomen in de TPM('s).

Bij **carve-in** (de "all inclusive methodiek") doet de IT-auditor zelf onderzoek naar de mate waarin de serviceorganisatie voldoet aan de eisen met betrekking tot informatieveiligheid.

Wat niet wijzigt is dat de gemeenten zich dus over het geheel verantwoorden. Dit betreft de werkzaamheden die in eigen beheer worden uitgevoerd én de verantwoording over de uitbestede taken.

1.2. Wel of geen TPM?

Werken met een TPM is niet verplicht. Dit geldt voor DigiD in gelijke mate als voor de toetsing van Suwinet in geval van uitbesteding. Wel dient het geheel van de criteria en controls te worden afgedekt in de collegeverklaring voor verantwoording. Dit gebeurt of door het assessment op de collegeverklaring van de eigen IT-auditor of door het oordeel in de ontvangen TPM('s) van de IT-auditor van de serviceorganisatie(s).

---

[1] Assertion based betekent dat de verantwoording wordt afgelegd op basis van een verantwoordingsdocument van de opdrachtgever of partij die verantwoording aflegt. De resultante hiervan is een assurancerapport op basis van NOREA-Richtlijn 3000A (Assertion based).

De auditor van de collegeverklaring is wel verantwoordelijk voor het totale proces, om te controleren of het geheel van de te verantwoorden controls wordt afgedekt. De compleetheid moet worden gewaarborgd. De auditor van de collegeverklaring is niet verantwoordelijk voor de inhoudelijke uitvoering hiervan die wordt afgedekt door een TPM. In welke gevallen hiervoor gekozen kan worden en wat daarvan de consequenties zijn, wordt uitgelegd in hoofdstuk 2.

2. Samenwerkingsverbanden

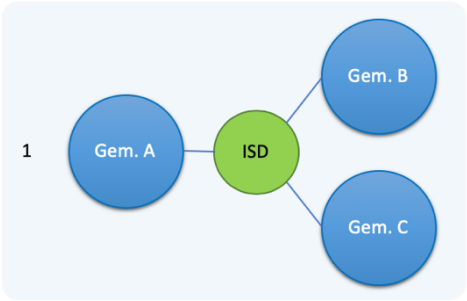
2.1. Samenwerkingsvormen

Of het raadzaam is om te werken met een TPM (het is namelijk niet verplicht) hangt af van de wijze waarop de uitvoering van de SUWI-taken en niet-SUWI-taken zijn ondergebracht bij serviceorganisaties. Wanneer gewerkt wordt met een TPM, dan wordt deze volgens de carve-out methodiek beoordeeld door de auditor van de collegeverklaring. De impact van de carve-out methodiek is uitgewerkt voor onderstaande vier typen van samenwerking binnen het Sociaal Domein (SD). Deze lijst van varianten is niet uitputtend.

1. Intergemeentelijke Sociale Diensten (ISD).
2. Uitvoering van Sociale Diensttaken vanuit een bedrijfsvoeringsorganisatie waarin twee of meer gemeenten participeren.
3. Gemeentelijke sociale dienst die voor één andere gemeente taken uitvoert.
4. Gemeentelijke sociale dienst die voor twee of meer gemeenten taken uitvoert.

1. Intergemeentelijke Sociale Diensten (ISD)

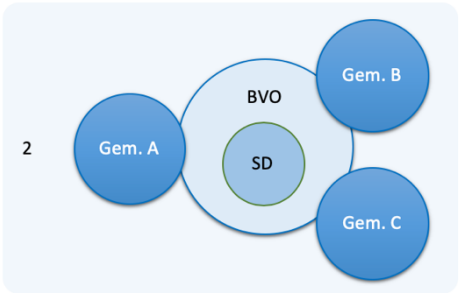
Een ISD is een organisatie die SD-werkzaamheden voor twee of meer deelnemende gemeenten uitvoert. Meestal staat een ISD juridisch op afstand van de deelnemende gemeenten: er is vaak sprake van gedelegeerd opdrachtgeverschap.



Het wordt aangeraden om de ISD voor 15 oktober een TPM op te laten leveren aan alle deelnemende gemeenten. De deelnemende gemeenten laten vervolgens in februari/maart de eigen collegeverklaring toetsen.

2. Uitvoering van SD-taken vanuit een bedrijfsvoeringsorganisatie (BVO) waarin twee of meer gemeenten participeren

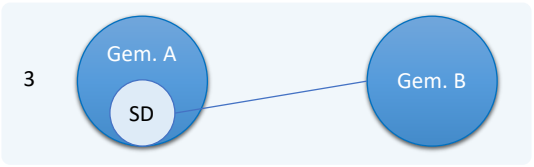
Er is sprake van een aparte organisatie (juridische entiteit) waarin de SD-taken van twee of meer gemeenten zijn ondergebracht. De bedrijfsvoeringsorganisatie voert vaak in mandaat werkzaamheden uit voor de aangesloten gemeenten.



In deze situatie is het te overwegen om voor alle gemeenten één en dezelfde auditor aan te stellen die de individuele collegeverklaringen van de gemeenten toetst. Deze collegeverklaringen zullen (nagenoeg) gelijk zijn. De aangesloten gemeenten nemen (voor alle gemeenten gelijk)

de uitkomsten voor de zelfevaluatie op in ENSIA voor 31 december. Eén auditor toetst in de verantwoordingsfase de collegeverklaringen in één keer voor de aangesloten gemeenten. De auditor hoeft immers maar één keer de opgenomen constateringen voor Suwinet te toetsen omdat deze gelijk zijn voor de aangesloten gemeenten binnen de bedrijfsvoeringsorganisatie.

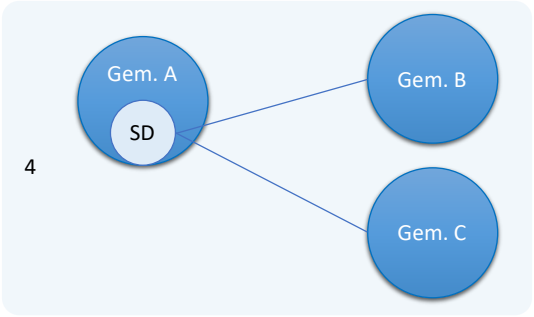
3. **Gemeentelijke sociale dienst die voor één andere gemeente taken uitvoert**
In deze situatie voert een gemeente SD-taken voor een andere gemeente uit. Deze gemeente fungeert als serviceorganisatie voor één andere gemeente.



Het advies is om één en dezelfde auditor de collegeverklaring voor beide gemeenten te laten toetsen. Er hoeft dan de facto geen TPM opgeleverd te worden wat de auditkosten beperkt tot het toetsen van de twee collegeverklaringen van elk van de gemeenten.

Werkwijze: Op basis van zelfassessment levert de uitvoerende gemeente de antwoorden voor de van toepassing zijnde controls/maatregelen voor 31 december op aan de opdrachtverstrekkende gemeente. De auditor toetst dan na januari de beide collegeverklaringen waarbij de verklaringen voor Suwinet bij de uitvoerende gemeente getoetst worden en dan ook gelden voor de opdrachtverstrekkende gemeente.

4. **Gemeentelijke sociale dienst die voor meerdere gemeenten taken uitvoert**
Afhankelijk van het aantal gemeenten waarvoor een gemeente SD-taken uitvoert, leidt dit tot de volgende twee scenario's.



a. De gemeentelijke sociale dienst levert een TPM op aan de opdrachtgevers (gemeenten) rond 15 oktober van een jaar. Alle gemeenten laten vervolgens individueel hun eigen collegeverklaring toetsen (naar model ISD). Dit betekent voor de gemeente die de dienstverlening levert dat deze twee audits laat uitvoeren, te weten één voor de TPM (september-oktober) en één voor haar eigen collegeverklaring (vanaf 1 januari).

b. De gemeentelijke sociale dienst levert de antwoorden voor Suwinet op basis van haar eigen zelfevaluatie voor 31 december aan de gemeenten waar zij diensten voor uitvoert, maar levert geen TPM op. Elke gemeente laat haar eigen collegeverklaring door de auditor toetsen. De auditors van de gemeenten waar diensten voor worden uitgevoerd zullen zelf onderzoek bij de serviceorganisatie (dienstverlenende gemeente) uitvoeren.

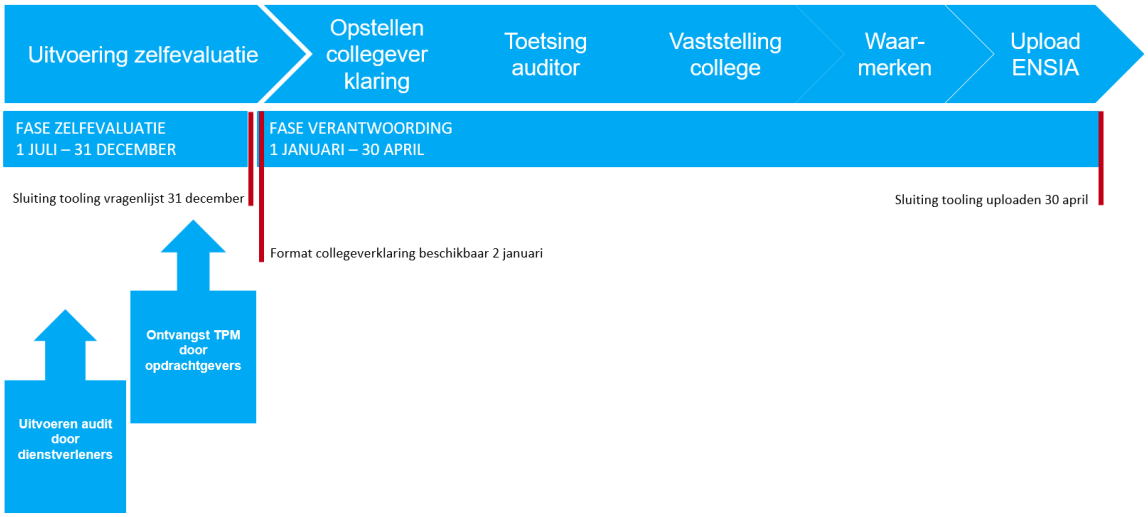
2.2. Opdrachtverstrekking en planning

Afhankelijk van de hierboven beschreven scenario's dient u mogelijk opdracht te verstrekken tot het afgeven van een TPM. Houdt er rekening mee dat voor het afgeven van een TPM de serviceorganisatie/leverancier kosten in rekening kan brengen. Vanuit de samenwerkingsvorm zult u hier wellicht aanvullende afspraken over moeten maken. NOREA heeft een format opgesteld voor de toetsing van Suwinet bij serviceorganisaties. Deze is gebaseerd op een ISA3000A-rapportage type 1: voor opzet en bestaan.

TPM's voor Suwinet moeten voor 15 oktober ontvangen zijn voor een tijdige verwerking in de ENSIA-zelfevaluatie van de opdrachtverstrekkende gemeente. Hiervoor geldt hetzelfde tijdpad als voor de ontvangst van de TPM's voor DigiD wordt gehanteerd. Er moet immers voldoende tijd te zijn voor opname van de uitkomsten in de eigen BIO-zelfevaluatie. Als tekortkomingen geconstateerd zijn, dan moet u afspraken maken over de uitvoering van de verbeteringen.

2.3. Verantwoordingsproces in ENSIA

In de periode 1 juli tot en met 31 december vindt de zelfevaluatie door de gemeente plaats. De informatie uit te ontvangen TPM's wordt door gemeenten verwerkt in hun zelfevaluatie. De vragenlijst moet volledig beantwoord zijn om deze uiterlijk voor 31 december af te kunnen sluiten (in ENSIA heet dit 'inleveren').



Per 2 januari zijn de formats voor de collegeverklaring beschikbaar. In bovenstaande tijdlijn zijn de activiteiten weergegeven. In tegenstelling tot de verantwoording DigiD hoeft u de ontvangen TPM's **niet** te uploaden in ENSIA. BKWI (de uitvoeringsorganisatie) en het ministerie van SZW steunen op de controlewerkzaamheden van uw auditor. Het is mogelijk dat voor onderzoek/verificatie u in een later stadium gevraagd wordt om alsnog een TPM te verzenden naar BWKI. Dit proces loopt buiten ENSIA om.

Bijlage A: Verantwoordingsrichtlijn GeVS 2022

Hoofdstuk	Nummer	Normen
5. Informatiebeveiligingsbeleid	5.1.1	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
	5.1.2	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
6. Organiseren van informatiebeveiliging	6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.
	6.1.2	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden informatiebeveiliging om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
7. Veilig personeel	7.2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
9. Toegangsbeveiliging	9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
	9.2.2	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
	9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
	9.2.6	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
10. Cryptografie	10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
12. Beveiliging bedrijfsvoering	12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.
	12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
	12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
18. Naleving	18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

Tabel: Scope van de verantwoording: normenkader GeVS (bron: BKWI, Verantwoordingsrichtlijn Informatie-beveiliging GeVS 2022 versie 1.0.pdf).