HANDREIKING Suwinet (in kader ENSIA) voor IT-auditors (RE's)

Versie 1.0 – 30 september 2026

Frequently Asked Questions – I d.d. 6 november 2026

Naar aanleiding van de publicatie van de Handreiking Suwinet (in kader ENSIA) voor IT-auditors (RE's) versie 1.0 d.d. 30 september 2026 is een aantal vragen ontvangen welke aanleiding geven tot nadere toelichting. De vraagstukken zijn hierna nader uitgewerkt.

Interpretatie werkzaamheden normen 9.2.5.3 en 12.4.1

In overleg en op initiatief van de VNG en in nauw overleg met het Ministerie van SZW / BKWI (stelselhouders/ beheerder / toezichthouder) is besloten tot een nadere invulling in afwijking van de beschreven beheersmaatregelen in de BIO 1.04.

Bij 9.2.5.3 is inderdaad de bedoeling dat de beheerder 4x per jaar (dus 1x per kwartaal) een controle uitvoert op alle gebruikers. De auditrespons is elk kwartaal 1 geval selecteren (dus een minimale selectie) en kijken of er sprake is van een de afwijking en of de afwijking als incident is behandeld en opgevolgd.

Bij 12.4.1 is het eveneens de bedoeling dat de testaanpak wordt gevolgd en daar staat 4x per jaar, eenmaal per kwartaal uitgaande van de werkzaamheden en verantwoordelijkheden van de organisatie.

Nuancering: Het is aan de auditor om te beoordelen of de organisatie een adequate interne controle uitvoert om de bedoelde punten. Centraal staan:

- Het voldoen aan de minimumeis van de BIO 1.04;
- Invulling geven aan de overeengekomen aanvullende eisen (met name het gespreid over het jaar, per kwartaal uitvoeren van specifieke controlewerkzaamheden). Hieronder valt bijvoorbeeld ook de werkwijze van een organisatie die per trimester een integrale controle op alle gebruikers uitvoert.
- De aantallen waarnemingen in het kader van de auditrespons dient minimaal te voldoen aan de uitgangspunten verwoord in bijlage 3 van de Handreiking.
- De onder 9.2.5.3 en 12.4.1 vermelde uitwerking is als wenselijke benadering uitgewerkt. De auditor dient te bevorderen dat verantwoordelijke partijen hieraan gericht invulling geven. Bij een lagere frequentie aan controles dan vier per jaar laat de opvolging van de resultaten zoals bij voorbeeld onrechtmatige raadpleging lang op zich wachten en daarom is er -afwijkend van de BIO 1.04- voor een kwartaal controle gekozen. Gezien echter het late tijdstip van bekendmaking kan voor verantwoordingsjaar 2026 tijdelijk worden volstaan met een frequentie van 2 interne controle per jaar conform de tekst van Bio 1.04.

Controleperiode bij controle werking

Op dit punt zijn verschillende vragen ontvangen. Tegen deze achtergrond een uitgebreidere beantwoording.

<u>Wettelijk kader</u>

Voor Suwi-gerelateerde opdrachten omvat dit geheel de Wet Structuur Uitvoering Werk en Inkomen en de bijbehorende uitingen (Besluit SUWI / Regeling SUWI (art. 5.22 en 6.4) / Verantwoordingsrichtlijne GeVS).

Voor de werkzaamheden van de IT-auditor en meer in bijzonder die in het gemeentelijk domein (in den brede – dus ook keten) en bij de overige afnemers (denk aan UWV / SVB / etc.) is daarbij de Verantwoordingsrichtlijn GeVS (Gemeenschappelijke elektronische Voorzieningen SUWI) leidend. Hierin heeft de regelgever nader inhoud gegeven aan de verantwoordingsplicht die op de afnemer rust (verantwoording en daarbij door IT-auditor RE af te geven oordeel.

En voor de goede orde: de governancestructuur waarin de Verantwoordingsrichtlijn GeVS tot stand

komt is wettelijk verankerd en daarmee is de Verantwoordingsrichtlijn GeVS ook eenduidig wettelijk verankerd.

Controle werking gemeentelijk domein

In het kader van de discussie is de Verantwoordingsrichtlijn GeVS 2025 leidend. In de Verantwoordingsrichtlijn GeVS 2025 zijn als belangrijke issues vastgelegd:

a. Voor gemeentelijke afnemers: de overgang van verantwoording / toetsing over opzet / bestaan van maatregelen naar verantwoording / toetsing over opzet / bestaan en werking van maatregelen.

b. Voor gemeentelijke afnemers: een eenduidig pad bestaande uit 3 stappen:

    a. Voor het verantwoordingsjaar 2025 handhaven van verantwoording over opzet / bestaan

    b. Voor het verantwoordingsjaar 2026 introductie van verantwoording over opzet / bestaan / werking over een deel van de maatregelen

    c. Voor het verantwoordingsjaar 2027 introductie van verantwoording over opzet / bestaan / werking over het geheel van de maatregelen.

Daarmee heeft de regelgever mede invulling gegeven aan verzoeken van verantwoordingsplichtigen om voldoende voorbereidingstijd te krijgen op het geheel. Daarmee heeft de regelgever ook invulling gegeven aan adviezen van de zijde van NOREA inzake randvoorwaarden voor een goed verloop van het geheel.

Met dit pad kan er geen misverstand bestaan over de aard van de verantwoording over het verantwoordingsjaar ongeacht de partij die het betreft / de positie die de partij in de keten heeft.

En voor de volledigheid: met het verantwoordingsjaar wordt de gehele periode 1-1 t/m 31-12 bedoeld, hetgeen wil zeggen dat de controleperiode -afwijkend wat Logius voor DigiD heeft bepaald, voor Suwi het gehele jaar

Nadere informatie

Voor de goede orde nog even het volgende:

a. De Verantwoordingsrichtlijn GeVS 2026 (eind december 2025 vastgesteld en gepubliceerd) omvat geen inhoudelijke wijzigingen in het bovengenoemde traject / reikwijdte verantwoording maar was / is noodzakelijk om de besluitvorming in ENSIA-verband om over te gaan op assurance volgens 3000D (werkafspraak gemeentelijke afnemers / daarmee optie voor overige afnemers) te formaliseren.

b. De Verantwoordingsrichtlijn GeVS 2027 (medio 2026 vastgesteld en gepubliceerd) omvat geen inhoudelijke wijzigingen in het bovengenoemde traject / reikwijdte verantwoording maar is de opmaat voor de toepassing van BIO 2 versie 1.3 bij alle verantwoordingsplichtige afnemers.

c. Door het Ministerie van SZW / BKWI is aangegeven dat nu reeds gewerkt wordt aan de Verantwoordingsrichtlijn GeVS 2028. Dit ook tegen de achtergrond dat deze naar alle waarschijnlijkheid een aantal fundamentele wijzigingen met zich mee zul brengen. E.e.a. heeft ook ten doel dat alle betrokkenen (verantwoordingsplichtigen en auditors) tijdig kunnen inspelen op de hierbedoelde wijzigingen.

d. De NOREA Handreiking voor het verantwoordingsjaar 2025 speelt op de hiervoor geschetste ontwikkeling in. Hierbij verdienen de volgende punten nadruk:

    a. De verantwoording over 2025 was ‘klassiek’ ENSIA / opzet – bestaan en daarmee leidend voor gehele Handreiking.

    b. De veranderingen voor het jaar 2026 zijn vroegtijdig geadresseerd:

i. Door uitwerken van de Handreiking op het punt van de controle op werking voor die normen waar dit over 2026 van kracht zou worden (en nu is).

ii. Door te proefaudits te faciliteren voor gemeentelijke afnemers die dit wilden:

1. Met nadrukkelijk de vermelding dat de rapportages uitsluitend voor de gemeenten (gemeentelijke keten) bedoeld waren en dat BKWI / SZW deze niet wilden / hoefden te zien in het kader van hun toezichtsactiviteiten)

2. En de opname van de periode 6 maanden

3. En de afgrenzing op DKD

– beide (2 en 3) uit pragmatische overwegingen gelet op tijdstip beschikbaar komen Verantwoordingsrichtlijn GeVS / Handreiking 2025.

e. In het kader van het tot stand brengen van de NOREA Handreiking 2026 is het volgende ook nog van belang:

a. Zoals in 2025 al aangegeven (opleidingsactiviteit najaar 2025) werkt NOREA aan overdracht van verantwoordelijkheden voor opstellen van de Handreikingen naar stelselhouders omdat deze feitelijk daar beter thuishoren (namelijk toepassing van algemene regelgeving op specifieke regelgeving waarbij de beoogd (hoofd-) gebruiker mede aard / diepgang werkzaamheden bepaald. Daarmee is aanduiding Controleprotocol voor de Handreiking een beter begrip.

Als eerste stap is daar voor de Handreiking 2026 ook het pad belopen van advies door Domeingroep Privacy en Beveiliging en vaststelling door Managementoverleg Afspraken en Voorzieningen (governanceorganen SZW zoals hiervoor bedoeld). Daarmee heeft de Handreiking 2026 ook een wettelijk verankerde status gekregen.

b. In het kader van de uitwerking ervan heeft intensief overleg met SZW plaatsgevonden over een aantal aspecten:

i. (Her-) bevestiging verantwoordingsperiode voor alle actoren: GeVS geeft pad en dus is verantwoordingsperiode 1-1 / 31-12;

ii. Mede op basis van waarschuwingen van NOREA-zijde gebaseerd op observaties in de praktijk ten aanzien van stand van zaken opzet / bestaan / werking en de verwachting dat dit 'negatiever' zal uitvallen dan gewenst (gelet ook op gehanteerde overgangstermijn) met nadruk ook de aanscherping om in de rapportages (daarmee ook 3000D) scherp onderscheid te maken tussen bevindingen ten aanzien van opzet / bestaan en werking anderzijds. Dit maakt helderheid rapportage SZW – via minister aan Tweede Kamer mogelijk.

iii. In dat kader ook gesproken op keteneffecten: SZW / BKWI streven in dit kader naar transparantie: maak inzichtelijk en afnemer dient te verantwoorden – zie hiervoor onder i en ii.

Samenvattend: verantwoording en assurance dienen op basis gehele verslagjaar 2026 (1/1 t/m 31-12 plaats te vinden.

.