

Check-IN
tbv **PE-punten** voor
Actualiteiten DigiD, Suwinet
en ENSIA 30 september 2026



NOREA 
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Actualiteiten DigiD, Suwi(-net) en ENSIA

2026 en verder
“De rol van de IT-auditor belicht”

Actualiteiten DigiD, Suwinet en ENSIA 30 september 2026

Agenda – deel II

 13:30 – 14:00: Inloop en registratie

 14:00 – 14:05 Opening
Boris Scheepers en Jan Roodnat

 14:05 – 14:15 Toelichting Bestuur NOREA
Marc Welters

 14:15 – 15:00 DigiD actualiteiten
Jorik van 't Hof en Jacko Möhle

 15:00 – 15:15 Pauze

Agenda – deel II



15:15 – 16:00 Suwi actualiteiten
Nina Zaijjer, Milan Kaihatu en Peter Verstege



16:00 – 17:00 ENSIA – toekomst
Frank Heijligers / Monique Bos / Rob van Linden /
Rob Polderman en Jan Roodnat



17:00 – 17:10 Vragen staat vrij!
Jan Roodnat i.s.m. sprekers



17:10 Afsluiting en netwerkborrel
Jan Roodnat

Opening

Boris Scheepers en Jan Roodnat
(NOREA)

Actualiteiten DigiD, Suwinet en ENSIA 30 september 2026

Huishoudelijke mededelingen



Registratie – scannen QR-code/ formele toekenning PE-punten



Opname

- Ten behoeve: afwezig
- Latere terugkoppeling op besproken vraagstukken



Telefoon stil



Strak schema / vol programma



Evaluatieformulier = basis PE-punten



Netwerkborrel = ontmoeten

Toelichting door het bestuur van NOREA

Marc Welters

Actualiteiten DigiD, Suwinet en ENSIA 30 september 2026

DigiD actualiteiten

Jorik van 't Hof en Jacko Möhle

Actualiteiten DigiD, Suwinet en ENSIA 30 september 2026

Agenda

Terugblik op verantwoordingsjaar 2025

Ervaringen en afronding van ENSIA voor DigiD

Handreiking en rapportagetemplate 2026

Wijzigingen en gevolgen voor de auditpraktijk

Vooruitblik

Toezicht, precheck en vragen

Terugblik op verantwoordingsjaar 2025

Scope te breed of te smal

Verschillende interpretaties van de grenzen van het onderzoeksobject

Afwijkingen van user controls

De afwijking ten opzichte van het RSO vraagt een toelichting

Verschillende softwareversies

De dienstverlener gebruikte soms een oudere versie dan de versie in het RSO

Hertoetsen op werking

Soms vrijwel dezelfde controleperiode als bij de eerdere toets

Uitsluitend directe opdrachten

2025

3000A nog toegestaan voor gemeenten binnen ENSIA, inlevering januari–mei 2026

2026

De ENSIA–uitzondering vervalt uit de handreiking. Alle DigiD–assessments volgens 3000D

Wat blijft

Normenkader 3.0 met 21 normen. Vijf normen ook op werking

Scope vanuit de gebruikersreis

Gebruikersomgeving

Vanaf het vroegste moment van gegevens invullen of DigiD-inlog, tot het beëindigen van de dienst

Invloedssfeer

Ook beheer, CI/CD, IAM, hosting en voorzieningen die de omgeving kunnen wijzigen

Koppelvlakken

Alle gegevensstromen van en naar de gebruikersomgeving meenemen

Technische uitwerking in bijlage 3

U/TV.01 MFA bij kritisch beheer

Explicieter waar sterke authenticatie nodig is, ook achter de toegang tot de kantooromgeving

U/PW.03 Webserver en API's

Aangescherpte CSP-tekst

Cloudomgevingen

Meer uitwerking van beheer, netwerkgrenzen en gedeelde verantwoordelijkheden

C.03 Kwetsbaarhedenbeheer

Aanleiding uit de praktijk

Wanneer was kwetsbaarhedenbeheer afdoende? De eerdere toelichting liet ruimte voor interpretatie

Duidelijker verwachtingen

De handreiking concretiseert de scanfrequentie en de opvolging naar ernst van de kwetsbaarheid

Gevolg voor de auditor

Beoordelen of analyse, opvolging en vastlegging samen een afdoend proces vormen

C.09 Patchen tot in productie

Meer expliciete componenten

Dependencies, PaaS, container images, hosts en Kubernetes-versies

Aantoonbare uitrol

Bijgewerkte code of images moeten ook in productie zijn gedeployed

Afhankelijkheid van de platformleverancier

Actualisatie verzoeken. Bij objectieve onmogelijkheid: contextspecifieke verklaring over niet-exploiteerbaarheid

Steunen op serviceorganisaties

Productieversie en RSO moeten aansluiten

De gebruikte versie mag niet ouder zijn dan de versie waarop het RSO betrekking heeft

Afwijken van user controls toelichten

Afstemmen met de RSO-auditor. Dooruitbesteding expliciet zichtbaar maken

Wat verandert in het rapport?

Een eigen beschrijving van het onderzoeksobject

Vanuit de dienstverlener, per applicatie en met de gebruikte versie

Non-occurrence bij bestaan

Voldoet in opzet, met geen oordeel over bestaan in de toelichting

Her-assessment en deeltoets

Gericht op het eerdere gebrek

Een deeltoets is toegestaan, dus niet altijd de gehele norm te toetsen.

Hertoets op werking

Minimaal zes maanden, vanaf herstel van de eerdere omissie

Ingangsdatum

Versie 2026 vanaf 1 oktober 2026

Bepalend is de oordeelsdatum voor opzet en bestaan

Vooruitblik

Toezicht en opvolging

Verscherpt toezicht en herstel van tekortkomingen

Precheck

Plaats in het proces en verwachtingen aan de auditor

Komende assessmentperiode

Pauze

15:00 – 15:15 Kort maar krachtig

Actualiteiten DigiD, Suwinet en ENSIA 30 september 2026

Suwi actualiteiten

Nina Zaaijer, Milan Kaihatu en Peter Verstege

Actualiteiten DigiD, Suwinet en ENSIA 30 september 2026

Agenda

 Van Handreiking naar Controleprotocol

 Handreikingen Verantwoordingsjaar 2026

 Besluiten en lopende acties

Van Handreiking naar Controleprotocol - I



NOREA:

– Vaktechnische uitingen:

- Richtlijn: status – comply
voorbeeld: Richtlijn assurance-opdrachten (3000, Attest- en Directe Opdrachten)
- Handreiking: status – comply or explain
Voorbeeld: Handreiking Opdrachtgerichte Kwaliteitsbeoordeling (OKB)
Voorbeeld: Handreiking ENSIA
- Studie: status – neem kennis van
Voorbeeld: Wetgevingsoverzicht / Legislative Overview

Van Handreiking naar Controleprotocol - II



Controleprotocol:

- Onderdeel van regelgeving (PM: ook privaatrechtelijke overeenkomsten) rond verantwoording en controle
- Controleprotocol: specificatie specifiek uit te voeren assurance-werkzaamheden / formats assurance-rapportages ('oordeel')
- Beheerverantwoordelijkheid: regelgever (stelselhouder / stelselbeheerder / toezichthouder / governance regelgever leidend)
- Rol NOREA: toets op uitvoerbaarheid
 - Positief: status Handreiking
 - Negatief: advies ter verbetering (wet- en regelgeving en / of verantwoording en / of assurance (-werkzaamheden))

Van Handreiking naar Controleprotocol SUWI

Stap 1: Overdracht verantwoordelijkheid

- Werkzaamheden: NOREA Werkgroep i.s.m. SZW / BKWI
- Governance NOREA: Werkgroep / Vaktechnische Commissie / Bestuur
- Governance SUWI: Domeingroep Privacy & Beveiliging (DPB) / Managementoverleg Afspraken & Voorzieningen (MAV)

Stap 2: Werkzaamheden onder directe aansturing SZW / BKWI

- Werkzaamheden: warme overdracht
- Governance SUWI: DPB / MAV
- Governance NOREA: toetsing Werkgroep / (VC) / Bestuur

Van Handreiking naar Controleprotocol SUWI



Stap 3: “Alles in 1 hand” – SZW/BKWI aan het stuur

- Vertaling wet- en regelgeving naar verantwoordings- en controleverplichtingen
- Controleprotocol (Handreiking) in eigen beheer inclusief
- Afstemming uitvoeringsproblemen
- NOREA is toetsende rol (“uitvoerbaarheidstoets”)

Handreiking SUWI (gemeenten) 2026

Uitdagingen - I

 Besluiten governance-organen ENSIA:

- Geen Collegeverklaring (met bijlagen DigiD / SUWI) en assurance-rapport (3000A)
- Losse verantwoordingen DigiD / SUWI
 - Verantwoording DigiD – conform regelgeving 3000D
 - Verantwoording SUWI – van 3000A naar 3000D

 **IMPACT HANDREIKING:**

- Groot – gehele hoofdtekst herzien
- Groot – nieuw format assurance-rapport dat voldoet aan informatiebehoeften SZW/BKWI enerzijds – Gemeenten anderzijds

Handreiking SUWI (gemeenten) 2026

Uitdagingen - II



Verbreiding verantwoording

- opzet / bestaan volledige normenset
- Werking: beperkt aantal normen



IMPACT HANDREIKING:

- Beperkt: Handreiking 2025 voorzag in 'proefaudit' op werking met handreiking
- Meegenomen:
 - Volledige set regelgeving in kader waarvan gebruik Suwinet is toegestaan
 - Afstemming SZW/BKWI/VNG
 - Strikter op aantal 'waarnemingen'
 - Omgaan met 'non-occurrence'

Handreiking SUWI (gemeenten) 2026

Uitdagingen - III

 Overgang BIO 1.04 naar BIO 2 versie 1.3:

- Uitzondering gemeenten voor verslagjaar 2026 (vaststelling en besluitvorming vrijwillige zelfregulering 2025)
- Doorzicht naar verantwoordingsjaar 2027:
 - BIO 2 versie 1.3
 - Alle normen opzet/bestaan en werking

 **IMPACT HANDREIKING:**

- Beperkt:
 - Handreiking 2026 sluit aan op Verantwoordingsrichtlijnen GeVS 2026
 - GeVS 2027 – indicatie veranderingen
- Informatie Taskforce BIO NOREA: onderliggende werkzaamheden veranderen wel / nog niet meegenomen / 1 slag op alle bestaande Handreikingen in overleg met stakeholders
- Waarschuwing: implementatie BIO 2 versie 1.3 verloopt moeizaam (Risico gebaseerde invulling / onvolledige implementatie BIO 1.04 / etc.)

Handreiking SUWI (overage afnemers) 2026

Uitdagingen



Invoegen optie 3000D naast 3000A

- Zie voorgaande slides – impact vermijden)
- Voorkeursoptie 3000A (dringend advies DPB aan MAV – continuïteit)



BIO 2 versie 1.3 verplicht:

- Basis besluitvorming 2025
- Basis publicatie maart 2026
- Basis Cbw augustus 2026



Impact Handreiking groot:

- Verwerken optie ‘lastig’ – veel overlaten aan auditor / verwijzen naar gemeenten
- Verwerken BIO 2 versie 1.3 is meer dan alleen omnummeren (‘devil is in the detail’)

Toelichtingen



GeVS 2026 en gemeenten



GeVS 2027 alle verantwoordingsplichtigen (BIO 2 versie 1.3)



Specifieke details testaanpak / oordeelsvorming



Oordeelsvorming



Aanleveren verantwoordingen

Verantwoordingsrichtlijn GeVS 2026 – Gemeenten 2026

Norm	Opzet	Bestaan	Werking per 2026	Werking per 2027
5.1.1	V	V	O	V
5.1.2	V	V	O	V
6.1.1	V	V	O	V
6.1.2	V	V	V	V
7.2.2	V	V	V	V
9.2.1	V	V	V	V
9.2.2	V	V	V	V
9.2.5	V	V	V	V
9.2.6	V	V	V	V
10.1.1	V	V	O	V
12.1.1	V	V	O	V
12.1.2	V	V	O	V
12.1.4	V	V	O	V
12.4.1	V	V	V	V
12.4.2	V	V	O	V
18.1.4	V	V	O	V

Verantwoordingsrichtlijn GeVS 2027 – Alle verantwoordingsplichtigen

Norm	BIO 2 v1.3	Opzet	Bestaan	Werking per 2027
5.1.1	5.01	V	V	V
5.1.2	5.01	V	V	V
6.1.1	5.02	V	V	V
6.1.2	5.03	V	V	V
7.2.2	6.03	V	V	V
9.2.1	5.16	V	V	V
9.2.2	5.18	V	V	V
9.2.5	5.18	V	V	V
9.2.6	5.18	V	V	V
10.1.1	8.24	V	V	V
12.1.1	5.37	V	V	V
12.1.2	8.32	V	V	V
12.1.4	8.31	V	V	V
12.4.1	8.15	V	V	V
12.4.2	8.15	V	V	V
18.1.4	5.34	V	V	V

Specifieke details testaanpak / oordeelvorming



Testaanpak (alle partijen):

- BIO – aantal maatregelen toets werking gedefinieerd als 1 x per jaar
- In overleg tussen VNG – SZW/BKWI – NOREA:
 - Interne controle: minimaal 4 keer gespreid over jaar
 - Testwerkzaamheden: minimaal 2 waarnemingen (conform tabel)
- Ook element inbreng bij evaluatiesessies BIO 2 BZK



'0 – Occurance' (alle partijen):

- Aantal normen waar mogelijkheid waarnemen beperkt kan zijn in kader toetsen bestaan / werking
- Handelwijze 3000A (bijlage normhandhaving)
- Handelwijze 3000D (oordeelvorming per norm)

Oordeelsvorming



3000D (gemeenten):

- Basisinformatie toezichthouders (SZW / BKWI):
 - Oordeel opzet / bestaan norm (t.b.v. continuïteit samenvattende toezichtsrapportage)
 - Oordeel werking (inzichtelijk maken groeipad)
- Basisinformatie gemeenten:
 - Keten ('dienstverleners' / 'samenwerkingspartijen')
 - Toepassingen (conform overzicht toegelaten gebruik Suwinet)



3000A (overige)

- Bijlage normnaleving aangescherpt (opzet/bestaan – werking)

Aanleveren verantwoordingen



Gemeente (afnemer) blijft verantwoordelijk voor gebruik

- In kader interventieprotocol ook aanspreekpunt voor SZW / BKWI (Toezicht)



Aanleveren bij volledige uitbesteding (gemeenten):

- Gemeenten verantwoordelijk voor aantoonbaar zijn volledige uitbesteding van werkzaamheden (= gebruik suwinet-faciliteiten)
- Volstaan kan worden met assurance-rapport (3000D) dienstverlener / samenwerkingspartij mits uit rapport is af te leiden dat rapport (mede) voor gemeente bestemd is (zie format)
- Eenduidige aanlevering door / namens gemeente (aanbiedingsbrief)



Aanleveren bij BKWI:

- Sterke voorkeur via ENSIA-tooling
- Voordeel voor BKWI – geautomatiseerde overdracht tussen systemen – wegnemen van aantal handmatige slagen

Uitdagingen 2026 en verder



Alle organisaties:

- Implementatie BIO 2 v1.3
- Toenemend belang maar ook complexiteit informatieveiligheid



Cyberbeveiligingswet:

- Stelselniveau: Toezichtsregiem / toezichtsarrangementen
- Organisaties: ketenverantwoordelijkheden



SZW/BKWI en NOREA:

- Integratie Handreikingen – een generieke Handreiking SUWI?

In 2028 wijzigt mogelijk het normenkader van de Verantwoordingsrichtlijn GeVS



Domeingroep Privacy en Beveiliging (DPB) stelt een nieuw normenkader voor:

- Op basis van een risicoanalyse op het object Suwinet
- Ontwikkelingen op het gebied van wet- en regelgeving



DPB koppelt nieuw normenkader aan Verantwoordingsrichtlijn GeVS 2028.

- Verantwoordingsrichtlijnen 2026 en 2027 zijn reeds gepubliceerd.



Managementoverleg Afspraken en Voorzieningen (MAV) stelt de Verantwoordingsrichtlijn 2028 vast. Het streven is om dit in maart 2027 of eerder te doen.

ENSIA toekomst

Frank Heijligers / Monique Bos / Rob van Linden /
Rob Polderman en Jan Roodnat

Actualiteiten DigiD, Suwinet en ENSIA 30 september 2026

1. Wat gaat de Cbw voor ons betekenen?

2. Ervaren jullie een versnipperde verantwoording over beveiliging en digitalisering?

3. Hoe kom je tot een geïntegreerde verantwoording over beveiliging en digitalisering?

4. Hoe past ENSIA in SISA en een geïntegreerde verantwoording?

5. Hoe zou je de betrokkenheid van bestuurders bij beveiliging en digitalisering kunnen verhogen?

Vragen staat vrij!

Interactie sprekers – zaal

Jan Roodnat

Actualiteiten DigiD, Suwinet en ENSIA 30 september 2026

Afsluiting en netwerkborrel

Actualiteiten DigiD, Suwinet en ENSIA 30 september 2026

Bedankt

Voor meer informatie kun je contact opnemen met:

Jan Roodnat / Peter Verstege/ Jacko Möhle

06 – 18 30 42 36 / 06 – 53 71 63 09/ 06 – 43639816

j.roodnat@minfin.nl / pverstege@deloitte.nl / j.mohle@dbaudit.nl

© NOREA

Actualiteiten DigiD, Suwinet en ENSIA 30 september 2026

Check-OUT
tbv **PE-punten** voor
Actualiteiten DigiD, Suwinet
en ENSIA 30 september 2026



NOREA 
DE BEROEPSORGANISATIE VAN IT-AUDITORS