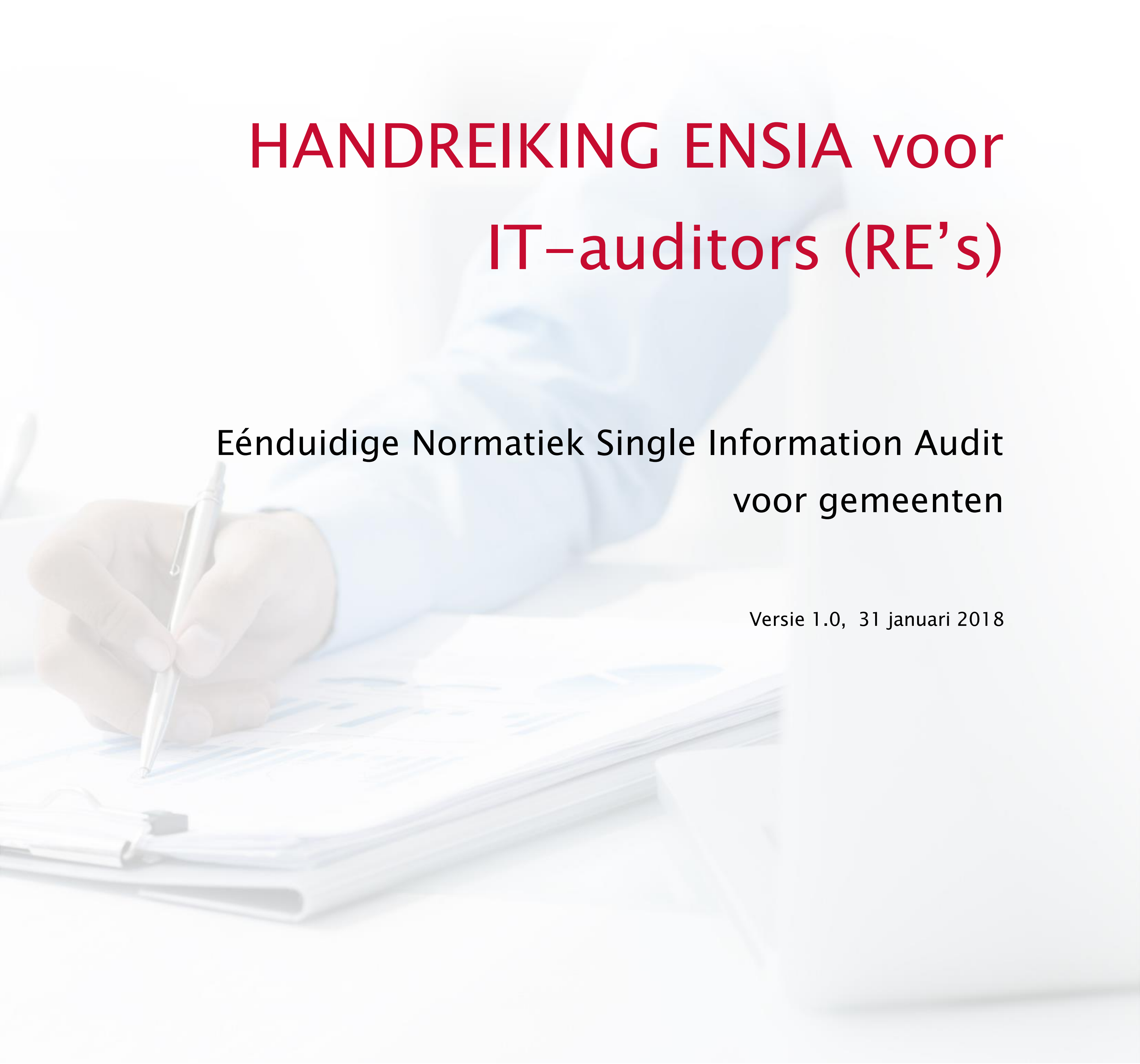
DE BEROEPSORGANISATIE VAN IT-AUDITORS



HANDREIKING ENSIA voor IT-auditors (RE's)

Eénduidige Normatiek Single Information Audit voor gemeenten

Versie 1.0, 31 januari 2018

Inhoud

Over deze handreiking ENSIA

Beheer

Deze handreiking is uitgegeven door NOREA, de beroepsorganisatie van IT-auditors in Nederland en is bedoeld als guidance-document voor de IT-auditors die zich bezighouden met het project Eénduidige Normatiek Single Information Audit (ENSIA) voor gemeenten.

De handreiking is afgestemd op de Notitie verantwoordingsstelsel ENSIA (versie 21 december 2017), zoals vastgesteld in het overleg met de ENSIA-Stuurgroep (Ministerie BZK). In die notitie is het format voor de bijlagen 1 (DigiD) en 2 (Suwinet) opgenomen, waarover in deze handreiking ‘guidance’ wordt geboden.

De handreiking mag worden gebruikt en/of gedistribueerd, mits met bronvermelding.

Voor vragen en opmerkingen kunt u zich wenden tot:

NOREA
Postbus 7984,
1008 AD Amsterdam
telefoon: 020-3010380
e-mail: norea@norea.nl

Meer informatie kunt u vinden op: www.norea.nl en/of www.ensia.nl

Deze ENSIA (concept-)handreiking zal op basis van de zelfevaluatie en proefaudit(s) door de ENSIA-Werkgroep van NOREA worden geëvalueerd en zo nodig verbeterd. Het is de bedoeling om de (concept-)handreiking op basis van ervaring en evaluatie als NOREA-handreiking (conform artikel 15 Reglement Beroepsbeoefening) vast te stellen.

Versiebeheer

Versie 0.9	30 oktober 2017	t.b.v. de ENSIA-training
Versie 0.91	16 november 2017	t.b.v. werkgroep ENSIA
Versie 0.92	21 november 2017	t.b.v. werkgroep ENSIA
Versie 0.93	23 november 2017	t.b.v. werkgroep ENSIA / Vaktechnische Commissie / Bestuurlijk Overleg BZK - VNG - NOREA
Versie 0.94	5 december 2017	Incl. commentaar VC-NOREA /VNG/PWC
Versie 0.95 / Versie 1.0	15 december 2017 t/m 31 januari 2018	Enkele correcties en aanvullingen verwerk

Aanleiding

Per 1 juli 2017 is het project ENSIA (Eénduidige Normatiek Single Information Audit) voor gemeenten van start gegaan. ENSIA is een gezamenlijk project van het ministerie van Binnenlandse Zaken (BZK), gemeenten, het ministerie van Sociale Zaken en Werkgelegenheid (SZW), het ministerie van Infrastructuur en Milieu (I&M) en de Vereniging Nederlandse Gemeenten (VNG). Het project heeft tot doel invulling te geven aan de verantwoordelijkheid van gemeenten rond informatieveiligheid.

De invoering van ENSIA betekent dat alle gemeenten vanaf 2017 werken met één verantwoordingsstelsel voor informatieveiligheid, waarbij over 2017 verantwoording wordt afgelegd over DigiD, Suwinet, de paspoortuitvoeringsregeling (PUN), de Basisregistratie Personen (BRP), de Basisregistratie Adressen en Gebouwen (BAG) en de Basisregistratie Grootschalige Topografie (BGT). De verantwoording sluit aan bij de gemeentelijke P&C-cyclus en is in lijn met de Baseline Informatieveiligheid Nederlandse Gemeenten (BIG).

Achtergrond

De kern van ENSIA is dat de gemeentelijke organisatie transparant is en verantwoording aflegt over de wijze waarop zij in control is op het thema ‘informatieveiligheid’. Die verantwoording legt de gemeentelijke organisatie af aan haar eigen toezichthouder, in casu de gemeenteraad. Gemeenten hebben over dit principe in de algemene ledenvergadering van de VNG van november 2013 overeenstemming bereikt.

Gemeenten leggen niet alleen verantwoording af aan de eigen toezichthouder. Van oudsher bestonden verplichtingen ten aanzien van het ministerie van BZK rond de Basisregistratie Personen (BPR), de PUN en DigiD, en het ministerie van IenW rond de BAG en de BGT. Naar aanleiding van de onderzoeken van de inspectie SZW is de regelgeving Suwinet aangescherpt en moeten gemeenten zich ook daarover verantwoorden.

ENSIA integreert al deze typen verantwoordingen in één werkwijze en met één eenduidige taal: de BIG. Alle bestaande verantwoordingen zijn in goed overleg met de toezichthouders aangepast op ENSIA. Voor alle verantwoordingen geldt dat waar mogelijk is aangesloten op de BIG. Specifieke toezichtinformatie is nodig en mogelijk verwerkt in de ENSIA-vragenlijst die de bevraagbare versie van de BIG als basis kent. Daarnaast blijft de noodzaak om domeinspecifieke toezichtinformatie te blijven leveren. Het idee is dat ENSIA de komende jaren met andere registraties verder zal worden uitgebreid.

Toepassingsgebied ENSIA

ENSIA is alleen van toepassing op gemeenten. De collegeverklaring gaat over DigiD en Suwi, waarbij de ENSIA-vragenlijst een breder perspectief heeft. Met ingang van 2017 gaat de DigiD-assessment voor gemeenten op in ENSIA. Daarnaast blijven in geval van nieuwe DigiD-aansluitingen de aansluitvoorwaarden van Logius ongewijzigd, waardoor binnen twee maanden na aansluiting ook voor gemeenten een reguliere DigiD-assessment moet worden uitgevoerd.

Met Suwinet wordt alleen gerefereerd aan de gemeente als afnemer. Als afnemer kent Suwinet ‘Suwi inkijk’, ‘Suwi inlezen’ en ‘Digitaal Klantdossier (DKD) inlezen’. Het specifieke normenkader Suwinet afnemers 2017 is de opvolger van de verantwoordingsrichtlijn Gezamenlijke elektronische Voorziening Suwi (GeVS). De methodiek is daarbij wezenlijk anders ingestoken, namelijk op basis van het onderkennen van een beleidsdomein, uitvoeringsdomein en control domein. De 13 generieke- en objectgerichte (BIG) controls van het Suwinet normenkader zijn uitgewerkt tot 11 ENSIA-normen voor Suwinet. Met de toezichthouder zijn afspraken gemaakt over het opnemen van de audit in ENSIA.

Werkwijze 2017

ENSIA ondersteunt zowel het horizontale als het verticale verantwoordingsproces. De ontwikkeling gaat daarbij steeds meer in de richting van horizontale verantwoording. Hieronder is het ENSIA-proces voor het verantwoordingsjaar 2017 grafisch weergegeven. Meer informatie omtrent ENSIA en de werkwijze is terug te vinden op www.ensia.nl.

HORIZONTAAL PROCES ENSIA VERANTWOORDING 2017

GEMEENTEN VERANTWOORDEN ZICH JAARLIJKS OVER HUN INFORMATIEVEILIGHEID.
DIT GEBEURT VANAF 2017 MET BEHULP VAN DE EENDUIDIGE NORMATIEK SINGLE INFORMATION AUDIT (ENSIA).

HET COLLEGE VAN B&W IS VERANTWOORDELIJK VOOR DE UITVOERING VAN HET ENSIA VERANTWOORDINGSPROCES.

1 JULI 2017

31 DECEMBER 2017

15 JULI 2018

ZELFEVALUATIE
Uitvoering zelfevaluatie informatieveiligheid.

OPSTELLEN
Opstellen paragraaf verantwoording informatieveiligheid.

VERANTWOORDEN
1. Verantwoording informatieveiligheid opnemen in jaarverslag.
2. Vaststellen van jaarverslag door college van b&w.
3. Goedkeuren van jaarverslag door de gemeenteraad.

OPSTUREN
Het college van b&w stuurt het gemeentelijk jaarverslag aan het ministerie van BZK.

Het horizontale verantwoordingsproces vormt een belangrijke basis voor de IT-auditor en de gemeente.

Het verticale verantwoordingsproces van de gemeente ziet er als volgt uit:


VERTICAAL PROCES VERANTWOORDING 2017

DE VRAGENLIJSTEN VOOR DE ZELFEVALUATIEPERIODE ZIJN TE VINDEN OP ENSIA.NL

1 JULI 2017

31 DECEMBER 2017 *

1 MEI 2018

ZELFEVALUATIE

1. Zelfevaluatie informatieveiligheid BRP, PUN, BAG, BGT, SUWInet.
2. Zelfevaluatie DigiD.

OPSTELLEN

Opstellen collegeverklaring over SUWInet en DigiD.

AUDIT

Audit over SUWInet en DigiD.

INLEVEREN

Inleveren collegeverklaring informatiebeveiliging, assurance rapport en TPM's.

* Informatieveiligheidsvragen lopen in 2017 mee met de planning van de Kwaliteitsmonitor van het ministerie van BZK. De vragenlijsten voor BRP en PUN via ENSIA.nl moeten daarom nog vóór 1 oktober 2017 worden ingeleverd.

Toelichting zelfevaluatie en tool gemeenten

Via de online ENSIA tool is er een zelfevaluatie vragenlijst beschikbaar voor informatieveiligheid bij gemeenten over de volle breedte van de BIG met inbegrip van de specifieke normen op het gebied van informatiebeveiliging van de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet). In vergelijking met de huidige situatie wordt het aantal vragen over informatieveiligheid met 15% gereduceerd.

Doel handreiking

Doel van deze handreiking is de IT-auditor een uniform toetsingskader te bieden voor het uitvoeren van een ENSIA-audit op basis van de beschikbare normen. Dit kader geldt voor controlejaar 2017. ENSIA-ontwikkelingen worden, indien nodig, vertaald in navolgende versies van deze handreiking. De handreiking biedt een richtinggevend referentiekader voor de werkzaamheden van de IT-auditor om hiermee te voorkomen dat er grote verschillen ontstaan in zowel de mate van diepgang bij uitvoering van de IT-audits, als bij het beoordelen van afwijkingen. Het is daarom uitdrukkelijk niet de bedoeling van deze handreiking voor de audit aanvullende vereisten op de geldende standaarden of aanvullende normen van bijvoorbeeld de NCSC-richtlijnen af te leiden.

Bij verschillen van inzicht is het primair aan de betrokken auditors om in overleg tot een oplossing te komen. De NOREA werkgroep ENSIA, of de werkgroep DigiD assessment kan daarbij eventueel als gesprekspartner deelnemen, altijd vanuit het perspectief van ENSIA (dus gericht op het geven van assurance). Voor substantiële meningsverschillen heeft de NOREA een procedure vastgesteld waarmee (via de Vaktechnische Commissie) een collegiaal standpunt wordt gegeven.

Verantwoordingsproces

Verantwoordelijkheden gemeente

In het kader van het ENSIA-verantwoordingsproces gelden de navolgende specifieke verantwoordelijkheden voor de gemeente:

- De gemeente is verantwoordelijk voor het uitvoeren van de zelfevaluatie per assessmentplichtige DigiD-aansluiting waarvan de gemeente de houder is. Voor DigiD-aansluitingen die op naam staan van samenwerkingsverbanden waaraan de gemeente deelneemt dienen de samenwerkingsverbanden zelfstandig de voorgeschreven DigiD-assessments per aansluiting te laten uitvoeren.

- Praktijk is dat de werkzaamheden in het domein werk en inkomen belegd kunnen zijn bij diverse samenwerkingsverbanden. Ongeacht de organisatie van de samenwerkingsverbanden blijft het gemeentebestuur verantwoordelijk voor het gebruik van Suwinet. De gemeente dient e.e.a. te betrekken in de zelfevaluatie. Zie bijlage 6 voor een nadere toelichting.

- Bij eventuele bevindingen in het kader van de zelfevaluatie dient de gemeente een verbeterplan op te stellen. Dit verbeterplan dient verbetermaatregelen te omvatten voor alle hiervoor bedoelde bevindingen.

Verantwoordingsproces in detail

Het verantwoordingsproces begint met het invullen van de zelfevaluatie vragenlijst informatiebeveiliging 2017. De vragenlijst informatiebeveiliging is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) aangevuld met vragen die wettelijk verplicht zijn voor PUN, BRP, Suwinet en BGT.

Voor DigiD is een aparte vragenlijst voor de zelfevaluatie beschikbaar. Per assessmentplichtige DigiD-aansluiting moet een vragenlijst worden ingevuld. In tegenstelling tot de andere wettelijke verplichtingen is DigiD namelijk te specifiek om in BIG normen te kunnen worden vervat (vertaald).

Voor alle vragen geldt dat de gemeente de ondersteunende assurance-informatie dient te verzamelen en gestructureerd toegankelijk dient te maken. Wat betreft de wijze van documentatie zijn aanwijzingen gegeven vanuit KING/VNG.

De gemeente heeft tot **31 december 2017** de tijd om de vragenlijsten in te vullen en in te leveren. Inleveren kan pas als alle vragen beantwoord zijn.

Ingeleverde vragenlijsten kunnen in principe niet meer worden gewijzigd. Indien bepaalde antwoorden toch nog veranderen dan dient de ENSIA-coördinator hiervoor contact op te nemen met de beheerder van het zelfevaluatietool (ICTU). Door tussenkomst van de beheerder kunnen naderhand wijzigingen worden doorgevoerd. Het spreekt voor zich dat dit terughoudend zal worden toegestaan.

Na invulling van de DigiD-vragenlijst per aansluiting dienen de uitkomsten door de gemeente te worden beoordeeld met inachtneming van de ontvangen assurance-rapporten (bekend als TPM-verklaringen). Deze beoordeling vindt plaats in de ENSIA-tool en leidt tot een daartoe opgenomen rapportageformat ‘Bijlage 1 DigiD’.

Voor Suwinet geldt een vergelijkbaar proces waarbij op basis van de antwoorden in de ENSIA tool een specifieke Suwinet-bijlage wordt gegenereerd. In tegenstelling tot DigiD worden bij Suwinet niet de van derden ontvangen assurance-rapporten (TPM’s) ter beschikking gesteld aan de toezichthouder.

Op basis van de uitkomsten van de zelfevaluatie wordt door de gemeente de Collegeverklaring Informatiebeveiliging opgesteld. In de collegeverklaring wordt - mede vanwege de vertrouwelijke aard van de informatie - een samenvatting van de bevindingen op hoofdlijnen opgenomen.

De Collegeverklaring Informatiebeveiliging en de hiervoor genoemde bijlagen vormen daarmee het object van controle voor de IT-auditor.

De gemeente levert voor 1 mei 2018 het assurance-rapport, de Collegeverklaring Informatiebeveiliging met bijbehorende bijlagen en de ontvangen assurance-rapporten (TPM’s) (alleen voor DigiD) op aan de toezichthouder. Deze documenten kunnen tot deze datum met behulp van het ENSIA-tool ter beschikking gesteld worden.

De IT-auditor dient er voor te zorgen dat de betreffende documenten door hem gewaarmerkt zijn en in de vorm van PDF-documenten beschikbaar zijn voor de gemeenten.

De IT-auditor dient bij de uitvoering van de werkzaamheden rekening te houden met de doorlooptijd van de formele behandeling van de Collegeverklaring Informatiebeveiliging (o.a. collegebehandeling, besprekingen met de raadscommissie(s) en gemeenteraad).

Nadere informatie over het verantwoordingsproces is opgenomen in de Handleiding ENSIA-tool voor gemeenten (zie www.ensia.nl).

Wat verandert er voor de IT-auditor

Voor de IT-auditor verandert ten aanzien van zijn verantwoordelijkheid voor het goed voorbereiden en inrichten van zijn controle in principe niets. Met dien verstande dat elk audit project om een specifieke voorbereiding vraagt waarbij rekening wordt gehouden met het onderscheid tussen ‘direct reporting’ en ‘attest’.

Bij de methode van ‘direct reporting’ (zoals bij de DigiD assessments gebruikelijk) is de IT-auditor zelf in ‘the lead’ en is voorbereiding in de vorm van het opvragen van stukken belangrijk.

Bij ENSIA is de oplevering thans in de vorm van een attest opdracht op basis van de collegeverklaring en bijlagen (‘assertion based audit’).

Hoewel de collegeverklaring het object van controle vormt, is de ingevulde en gedocumenteerde ENSIA tool voor de IT auditor het basismateriaal waar elke IT auditor vanuit kan en moet gaan. Op basis van de eigen risicoanalyse, zoals die voor elke audit project wordt uitgevoerd, stelt de IT auditor vast wat de diepgang van zijn werkzaamheden zullen zijn gegeven de veronderstelde kwaliteit van oplevering van de gegevensverzameling.

Het IT-audit project bestaat bij ENSIA met name ook uit het uitvoeren van procescontroles. De procescontroles geven de IT-auditor de mogelijkheid ook -en met name tussentijds- te beoordelen of de opgeleverde resultaten voldoen aan daaraan te stellen eisen. Daarbij valt te denken aan de authenticiteit van het aangereikte basismateriaal, de bruikbaarheid en de compleetheid van het aangereikte basismateriaal bij de onderscheiden onderdelen. In deze setting toetst de IT-auditor tussentijds en blijft objectief en onafhankelijk, terwijl de gemeente tijdig in de gelegenheid wordt gesteld verbeteringen door te voeren. De IT-auditor is daarbij niet inhoudelijk betrokken ter voorkoming van zelftoetsing.

Ook het aspect van risico-inschatting is van belang. Op basis hiervan bepaalt de auditor met welke diepgang de controles van de -door de gemeente in het kader van de self-assessment beoordeelde normen- moeten plaatsvinden.

Formele aspecten van de assurance-opdracht

Een ENSIA-audit betreft een assurance-opdracht met een redelijke mate van zekerheid, conform Richtlijn 3000 A(ttestopdracht). Het college van burgemeesters en wethouders komt met een collegeverklaring waarover de IT-auditor met redelijke mate van zekerheid assurance verschaft. Beoogde gebruikers van deze collegeverklaring en het oordeel van de IT-auditor zijn de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet.

Doel van de ENSIA-audit is het verkrijgen van voldoende geschikte assurance-informatie om een conclusie met redelijke mate van zekerheid te verschaffen of de collegeverklaring ENSIA 2017 inzake Informatiebeveiliging van DigiD en Suwinet (inclusief de bijlage 1 DigiD en de ENSIA bijlage voor Suwinet waarnaar in de collegeverklaring wordt verwezen) van de gemeente, in alle van materieel belang zijnde aspecten, juist is.

De criteria voor een ENSIA-audit betreffen de normen inzake DigiD (Norm ICT-beveiligings-assessments DigiD versie 2.0 op het openbare deel van de websites van het ministerie van BZK en de VNG) en Suwinet (verantwoordingsrichtlijn op website BKWI en notitie verantwoordings-stelsel op website ENSIA). De criteria worden ook in de collegeverklaring kenbaar gemaakt en zijn daarmee toegankelijk voor de gebruikers.

Het gaat om opzet en bestaan van de maatregelen per 31 december 2017. Er wordt geen oordeel gegeven over de werking van de maatregelen gedurende een periode. De NOREA hanteert het standpunt dat uitsluitend een herhaalde beoordeling van opzet en bestaan op den duur schijnzekerheid impliceert als niet ook de werking in de beoordeling wordt betrokken. Het invoeringstraject daarvan vraagt echter de nodige voorbereidingstijd. Vooralsnog blijft de ENSIA-audit over 2017 en 2018 beperkt tot op opzet en bestaan van de beheersmaatregelen.

Ethische voorschriften en beroepsregels

De IT-auditor dient het Reglement Gedragscode ('Code of Ethics') na te leven. Bij een actieve betrokkenheid bij de inrichting van of uitvoering bij informatiebeveiliging is dit een risico ten aanzien van het fundamentele beginsel objectiviteit (inclusief onafhankelijkheid). Idem voor actieve betrokkenheid bij de uitvoering van de self-assessment die door het college moet worden uitgevoerd.

Het uitvoeren van pre-audits en / of interim-controles zijn mogelijk en kunnen actief bijdragen aan een adequate uitwerking van de ENSIA-vragenlijsten en de bijbehorende onderbouwing.

Opdrachtaanvaarding en continuering

Vereisten vanuit de Richtlijn Opdrachtaanvaarding zijn onverkort van toepassing. Het object van onderzoek betreft informatiebeveiliging. Competentie en capaciteit van de IT-auditor op dit terrein is dan ook een randvoorwaarde. Ervaring met het uitvoering van DigiD-assessments en/of suwi-audits is daarbij wenselijk.

Kwaliteitsbeheersing

Het Reglement Kwaliteitsbeheersing NOREA (RKBN) is van toepassing, dit komt ook tot uitdrukking in het assurance-rapport. Gegeven de aard van de opdracht, het maatschappelijke belang en mogelijk brede verspreidingskring van de collegeverklaring en het assurance-rapport (o.a. als gevolg van de Wet openbaarheid van bestuur) is voor ENSIA-audits een opdrachtgerichte kwaliteitsbeoordeling (OKB) van toepassing. Hiervan kan in uitzonderingsgevallen worden afgeweken. De auditor dient de overwegingen ter zake in het dossier vast te leggen.

Risico-inschatting

De IT-auditor dient op basis van zijn inzicht risico’s op afwijkingen van materieel belang in de informatie over het onderzoeksobject te identificeren en in te schatten. De schaal van inschatting is Hoog, Midden of Laag. Een veel gebruikte benadering hierbij is die van het audit controle risico (ACR). Daarbij is het audit controle risico een product van Interne Controle Risico (ICR), Inherente Risico (IHR) en Detectierisico (DR). De ENSIA-opdracht is gezien het feit dat het de decentrale overheid betreft en het feit dat de opdracht als complex wordt aangemerkt, te bestempelen als een ‘high risk’ opdracht.

De ACR van deze opdracht wordt ‘laag’ verondersteld. Dat wil zeggen dat voorkomen moet worden dat ten onrechte een foutief oordeel wordt afgegeven.

- Inherente Risico: betreft een inschatting van de complexiteit van de te controleren objecten, in deze fase van release: DigiD en SuwiNet;

- Interne Controle Risico: betreft een inschatting van de kwaliteit van de beheersomgeving van de gemeente bij de totstandkoming van de collegeverklaring op basis van de zelfevaluatie en het proces van zelfevaluatie;

- Detectierisico: is de resultante en stelt eisen aan de kwaliteit van de eigen auditorganisatie en de aard en omvang van de controlewerkzaamheden om fouten (tijdig) te ontdekken.

Ten behoeve van het afgeven van het assurance-rapport dient het ACR laag te zijn. Omdat zowel ICR en IHR in de beginperiode op Midden tot Hoog worden ingeschat zal het DR Midden tot Laag moeten zijn. Dit betekent voor 2017 relatief nog veel uit te voeren controlewerkzaamheden in de vorm van gegevensgerichte maatregelen. Naar verwachting zal dit de komende jaren minder worden.

De auditor dient deze overwegingen ter zake vast te leggen in zijn dossier.

Het verkrijgen van assurance-informatie

De collegeverklaring komt tot stand doordat een self-assessment wordt uitgevoerd met behulp van de ENSIA tool. Dit biedt voor de IT-auditor een prima startpunt voor zijn audit. In beginsel is hierin de beoordeling vastgelegd met betrekking tot de individuele normen / vragen op basis van relevante assurance-informatie die door het college is verzameld. Deze assurance-informatie omvat ook voor de IT-auditor assurance-informatie voor zijn oordeel.

Een professioneel kritische houding wordt van de IT-auditor verwacht bij het gebruik van deze informatie. Om zelfstandig tot een oordeel te komen zal de IT-auditor niet alleen de uitvoering van de self-assessment beoordelen maar ook de onderliggende documentatie toetsen om zelfstandig te bepalen of in opzet en bestaan voldaan wordt aan de desbetreffende norm.

Gebruik van of steunen op de werkzaamheden van interne IT-auditors is mogelijk, met inachtneming van de vereisten zoals aangegeven in paragraaf 53-55 van Richtlijn 3000.

Onderdeel van de assurance-informatie is het verkrijgen van een schriftelijke bevestiging van de verantwoordelijke partij met een zo recent als mogelijke datum, voorafgaand aan de datum van het assurance-rapport. Deze omvat: een (her)bevestiging van de collegeverklaring dat toegang is verschaft tot relevante informatie en personen; geen kennis is van zaken die op het oordeel een ander licht werpen; alsmede een bevestiging omtrent gebeurtenissen na de periode of het tijdstip waarop de opdracht betrekking heeft.

Uitbesteding door gemeenten

Bij uitbesteding van werkzaamheden door gemeenten zijn de volgende situaties voorzien:

DigiD

Bij het beoordelen van uitbestede taken wordt aangesloten bij de in het kader van DigiD-assessments gebruikelijke werkwijze. Bij het beoordelen van uitbestede taken wordt uitgegaan van de ‘carve-out methode’. Hierbij ontvangt de houder (gemeente) een DigiD-assurance rapport van de externe partijen. De IT-auditor van de houder voert daarbij geen onderzoek uit naar de juistheid van de oordelen die zijn vermeld in de rapportage van de derde partijen en neemt ook geen verantwoordelijkheid voor de in die rapportage vermelde oordelen.

De IT-auditor verwijst in zijn oordeel naar de assurance-rapporten van derden voor de desbetreffende onderdelen

Binnen de ENSIA tooling zijn specifieke faciliteiten opgenomen om de betreffende documenten op te nemen en aan de toezichthouders ter beschikking te stellen.

Suwinet

SZW verwacht van gemeenten dat zij ook in het geval van uitbesteding en / of samenwerking met andere organisaties de bestuurlijke verantwoordelijkheid blijven nemen en daarover verantwoording afleggen.

Dit betekent dat de IT-auditor zich met betrekking tot Suwinet ook een oordeel moet vormen over de door de externe partijen uitgevoerde werkzaamheden en deze in zijn oordeelsvorming moet betrekken (‘inclusive benadering’).

Gebruik van of steunen op werkzaamheden van (interne) IT-auditors is mogelijk met inachtneming van de vereisten zoals aangegeven in paragraaf 53-55 van de Richtlijn 3000. Tevens zal de auditor daarbij aandacht moeten schenken aan de organisatie van de IT-audit (werkzaamheden), competentie van de verantwoordelijk IT-auditor en de geschiktheid van de uitgevoerde werkzaamheden in het kader van de ENSIA-audit.

Zie voor een nadere toelichting bijlage 6 “Overwegingen Audit in samenwerkingsverbanden Suwinet”. Het gaat hierbij om overwegingen die betrokken kunnen worden bij het uitvoeren van de werkzaamheden in de samenwerkingsverbanden. Deze mogen echter geen afbreuk doen aan de fundamentele eisen die aan het uitvoeren van de werkzaamheden door de IT-auditor zijn gesteld.

Werkzaamheden auditor

Bij uitbesteding door de gemeente aan een externe partij (samenwerkingsverband / externe leverancier / combinatie van beide) heeft het de voorkeur dat de externe partij een assurance-rapport (conform Richtlijn 3000 of ISAE 3402) verzorgt dat betrekking heeft op de in het kader van ENSIA gestelde normen.

Indien geen assurance-rapport geleverd kan worden dan wordt in opdracht van de gemeente bij de externe partij onderzoek gedaan naar de naleving van de in het kader van ENSIA gestelde normen. Dit kan door de gemeente zelf worden gedaan of door de auditor. Voorwaarde hiervoor is dat de ‘contractuele bepalingen’ tussen de gemeente en de externe partij dit onderzoek mogelijk maken.

De auditor van de gemeente dient hiervoor de vaktechnische verantwoordelijkheid te kunnen nemen. Hij dient dit – waar mogelijk in overleg met de auditor van de externe partij – te betrekken in de risico-analyse, uitwerking van de controle-aanpak, bespreking van bevindingen, etc. en uitvoering van een dossierreview. De inspanning zal beperkter kunnen zijn indien de auditor van de externe partij werkzaamheden conform de ENSIA-normering en deze handreiking uitvoert en in de rapportage een bijlage opneemt van de uitgevoerde werkzaamheden naar analogie van wat bij een 3402-rapportage type 2 vereist is.

De auditor dient de uitkomsten van de in dit kader uitgevoerde werkzaamheden te betrekken in zijn oordeelsvorming.

Het uiteindelijke streven moet zijn dat de externe partij(-en) een assurance-rapport (conform Richtlijn 3000) kan leveren. Een ISO 27001 rapport is voor het doel van ENSIA onvoldoende.

Verbeterplannen

Hoewel de IT-auditor geen oordeel geeft over de toereikendheid (en uitvoering) van het verbeterplan van de gemeente naar aanleiding van eventuele bevindingen in het kader van de zelfevaluatie, is het wenselijk dat hij verifieert of de door de gemeente gesignaleerde bevindingen geadresseerd zijn in het verbeterplan. Eventuele bevindingen dienen onder de aandacht van de opdrachtgever gebracht te worden zodat deze, onder verantwoordelijkheid van het College, betrokken worden in de uitwerking van het verbeterplan en, waar nodig, de collegeverklaring.

Schriftelijke bevestiging

Onderdeel van de assurance-informatie is het verkrijgen van een schriftelijke bevestiging van de verantwoordelijkge partij (gemeente) zo dicht als praktisch uitvoerbaar is bij, maar niet na, de datum van het assurance-rapport. Deze omvat:

- Een herbevestiging van de collegeverklaring;
- Een bevestiging dat toegang is verschaft tot relevante informatie en personen;
- Een bevestiging dat er geen kennis is van zaken die op het oordeel een ander licht werpen;
- Een bevestiging omtrent gebeurtenissen na de periode of het tijdstip waarop de opdracht betrekking heeft tot het moment van afgeven van de bevestiging die van invloed kunnen zijn op de collegeverklaring en de assurance die daarbij wordt afgegeven.

Het vormen van het oordeel

Bij het vormen van het oordeel worden de bepalingen uit het Stramien voor assurance-opdrachten in acht genomen zoals deze zijn vastgelegd voor attest-opdrachten (assertion-based opdrachten).

De beantwoording van de vraag of voldoende en geschikte controle-informatie is verkregen voor het oordeel blijft daarbij onderwerp van professionele oordeelsvorming. Indien onvoldoende en / of geen geschikte controle-informatie is verkregen brengt de IT-auditor dit tot uitdrukking in de strekking van het assurance-rapport (beperking of oordeelonthouding)

Omdat in de collegeverklaring eventueel melding wordt gedaan van verbeterplannen en de IT-auditor hierover geen assurance verschaft (‘Ons oordeel heeft zich niet gericht op deze verbeterplannen en het beleggen en monitoren hiervan’) is het wèl van belang om de eventuele verbeterplannen expliciet in de paragraaf ter benadrukking van aangelegenheden te benoemen.

In die gevallen waarin naar de mening van de IT-auditor de collegeverklaring en bijbehorende bijlagen een getrouw beeld geven van de informatiebeveiliging (rond DigiD en Suwinet) bij de gemeente maar de informatiebeveiliging gebreken vertoont, die op grond van de oordeelsvorming van de IT-auditor dermate belangrijk zijn dat ze fundamenteel zijn voor het begrip van de gebruikers van de collegeverklaring, brengt de IT-auditor in het assurance-rapport dit tot uitdrukking in een paragraaf ter benadrukking van aangelegenheden.

Het opstellen van het assurance-rapport

Voor de ENSIA-audit is gekozen voor een nieuwe structuur voor het assurance-rapport. Deze sluit aan op ontwikkelingen bij de NBA (Nederlandse Beroepsorganisatie van Accountants) en daarmee ook op ontwikkelingen in internationaal verband.

Het assurance-rapport kent de volgende indeling:

- Conclusie (het oordeel van de IT-auditor)
- Paragraaf ter benadrukking van aangelegenheden
- De basis voor de conclusie
- De verantwoordelijkheden van het management (gemeente)
- De verantwoordelijkheden van de IT-auditor
- Ondertekening

Bij het door de IT-auditor ondertekende assurance-rapport wordt ook de door de IT-auditor gewaarmerkte collegeverklaring en daarbij behorende bijlagen gevoegd. Deze set wordt door de gemeente gebruikt in het kader van het afleggen van verantwoording aan de toezichthouders (zie paragraaf Verantwoordingsproces). Het model assurance-rapport is opgenomen in bijlage 5.

Bij assurance-rapporten bij service-organisaties is het vereist dat bij het toetsen van de werking ook een bijlage wordt toegevoegd met een beschrijving van de uitgevoerde toetsingen van de interne beheersmaatregelen en de resultaten daarvan. De ENSIA-audit betreft een type 1 audit (opzet en bestaan). Daarnaast is het doel en de doelgroep anders dan bij een 3402-rapport. Het opnemen van een bijlage met de beschrijving van uitgevoerde werkzaamheden is dan ook niet verplicht, doch optioneel.

Als gerapporteerd wordt binnen een samenwerkingsverband waarbij andere auditors gebruik willen maken van de rapportage en de uitgevoerde werkzaamheden, dan wordt aangeraden wel zo’n bijlage toe te voegen om de afstemming van de verrichte werkzaamheden te faciliteren.

Documentatie

De IT-auditor dient tijdig opdrachtdocumentatie op te stellen die een vastlegging van de basis voor het assurance-rapport verschaft. Richtlijn Documentatie (230) is onverkort van toepassing (inclusief 60 dagen termijn). Het dossier van de IT-auditor is zelfstandig leesbaar. Een integrale verwijzing naar de zelfevaluatietool gehanteerd door het college is niet toegestaan.

Evenmin is een vastlegging door de IT-auditor in de ENSIA-tool en / of andere door de gemeente ten behoeve van het verzamelen en vastleggen van assurance-informatie gebruikte systemen toegestaan aangezien deze geïnterpreteerd kunnen worden als een (goedkeurend) oordeel met betrekking tot het betreffende deelonderwerp / vraag.

Tot slot

De ENSIA-audit maakt onderdeel uit van een breder overheidsinitiatief om de veiligheid van digitale dienstverlening te vergroten, maar is zeker niet het enige middel. Blijvende managementaandacht voor de risico's van digitale dienstverlening en het treffen van de juiste beheersmaatregelen is van groot belang. Algemeen geaccepteerde beheerskaders als ISO 27001/2 en de verschillende Baselines voor Informatiebeveiliging voor overheidsorganisaties. De IT-auditor betrekt deze context (de 'controle omgeving') wel bij zijn auditaanpak, maar voert daar in het kader van de ENSIA-audit geen specifiek onderzoek op uit.

Bijlage 1 Guidance bij de te onderzoeken normen DigiD

De testaanpak van de auditor is afhankelijk van de risicoanalyse

Tabel beveiligingsrichtlijnen met aandachtspunten (Richtlijnen uit: ICT-Beveiligingsrichtlijnen voor Webapplicaties. VERDIEPING. Nationaal Cyber Security Centrum. September 2015).

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld. Doelstelling: Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.	Governance	Betrokken partij(en): Applicatie-, hosting- of SAAS leverancier. Houder van de DigiD-aansluiting. Scope: De contracten en/of Service Level Agreements voor de levering hosting-, applicatie- of SAAS diensten. Nadere toelichting: De organisatie dient een, door beide partijen ondertekend, contract te hebben waarin tenminste de volgende zaken zijn opgenomen: een beschrijving van de te diensten die onder het contract vallen; de van toepassing zijnde leveringsvoorwaarden; informatiebeveiligingseisen met de relevante eisen vanuit het beveiligingsbeleid; het melden van beveiligingsincidenten en datalekken; de behandeling van gevoelige gegevens; wanneer en hoe de leverancier toegang tot de systemen / data van de gebruikersorganisatie mag hebben; Service Level Reporting; het jaarlijks uitvoeren van audits bij de leverancier(s); beding dat deze voorwaarden back-to-back worden doorgegeven aan mogelijke subleveranciers. Test aanpak: Interview de verantwoordelijke functionarissen.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			Inspectie van het beveiligingsbeleid. Inspectie van contracten met leveranciers, SLAs en andere gerelateerde documenten.
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken. Doelstelling: Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit.	Applicatie Infrastructuur Proces	Betrokken partij(en): Applicatie-, hosting- of SAAS leverancier. Houder van de DigiD-aansluiting. Scope: De DigiD webapplicatie, DigiD webservers en beheerinterfaces van de firewalls, routers, IDS/IPS, etc. Nadere toelichting: De focus ligt op de beheerprocessen. Dit betreft enerzijds toegang tot de DigiD-applicatie en anderzijds toegang tot de webservers die een koppeling hebben met de DigiD omgeving van Logius, de routers en de firewalls. Aandachtspunten hierbij zijn: Eisen aan wachtwoordinstellingen. Aantoonbare controle op joiners/movers/leavers. Wijzigen van de standaard wachtwoorden van administrator accounts. Beperken eventuele shared accounts. Uitvoeren periodieke reviews. Specifieke aandacht gaat uit naar wachtwoorden die leveranciers hebben om toegang tot de systemen of data van de houder van de DigiD aansluiting te krijgen (wie hebben die wachtwoorden, hoe worden die opgeslagen en wie hebben toegang. Hoe vaak worden ze gewijzigd, etc.). Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer het beveiligingsbeleid, joiners/movers/leavers procedure, de autorisatieprocedure, afspraken met leveranciers met betrekking tot toegang tot systemen en data en andere gerelateerde documenten. Stel voor elk van deze processen en systemen, het bestaan vast met een deelwaarneming van ten minste één.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. Doelstelling: Effectief en veilig realiseren van de dienstverlening.	Applicatie Proces	Betrokken partij(en): Applicatie of SAAS leverancier. Houder van de DigiD-aansluiting. Scope: De DigiD webapplicatie. Nadere toelichting: Deze norm richt zich meer op de procesmatige aspecten van het functioneel en het applicatiebeheer. Aandachtspunten hierbij zijn: Beschrijving van taken, verantwoordelijkheden en bevoegdheden van de verschillende beheerrollen. Autorisatiematrix waarin tot uitdrukking komt welke autorisaties aan welke beheerrollen (b.v. administrator, publicist, auteur, redacteur) worden toegekend. Autorisatiebeheerproces voor het onderhouden en toekennen van beheerrollen. Uitvoeren van een periodieke review. Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer de functie/taakbeschrijvingen van beheerders, de autorisatiematrix en het autorisatiebeheerproces. Inspecteer de toegekende autorisaties en de resultaten en opvolging van de periodieke review.
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt. Doelstelling: Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.	Applicatie	Betrokken partij(en): Applicatie- of SAAS leverancier. Scope: De DigiD webapplicatie en webserver. Nadere toelichting: Ongecontroleerde (ongevalideerde) invoer van gebruikers is een belangrijke dreiging voor een webapplicatie. Als invoer van gebruikers rechtstreeks wordt gebruikt in HTML-uitvoer, cookiewaarden, SQL-queries, etc., bestaat er een (grote) kans dat een kwaadwillende de webapplicatie compromitteert. Een gebrek aan

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			invoervalidatie kan tot kwetsbaarheden zoals XSS, commando- en SQL-injectie leiden. HTTP request voor alle invoermethodes zoals gespecificeerd in de ICT- Beveiligingsrichtlijnen van NCSC moeten worden gevalideerd (testen op type, lengte, formaat en karakters van invoer en speciale tekens (bv. <, >, ', ", & , /, --, etc.). Test aanpak: Om deze beveiligingsrichtlijn volledig te testen is een source code review nodig. Er is echter niet gekozen voor een verplichte code review als onderdeel van de DigiD assessment. Observeer het gedrag van de webapplicatie op ongeldige invoer. Voer hierbij een representatieve deelwaarneming uit op de invoermogelijkheden die de applicatie biedt.
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren. Doelstelling: Voorkom manipulatie van het systeem van andere gebruikers.	Applicatie	Betrokken partij(en): Applicatie- of SAAS leverancier. Scope: De DigiD webapplicatie. Nadere toelichting: Als een webapplicatie onvoldoende controles uitvoert op de uitvoer die het terugstuurt naar de gebruiker, kan het gebeuren dat er zich onbedoelde of ongewenste inhoud in de uitvoer bevindt. Uitvoervalidatie voorkomt dat de webapplicatie ongewenste opdrachten geeft aan de cliënt, bijvoorbeeld in het geval van XSS. De webapplicatie codeert dynamische onderdelen in de uitvoer waarbij mogelijke gevaarlijke tekens (bv. <, >, ', ", & , /, --, etc.) worden genormaliseerd. Test aanpak: Om deze beveiligingsrichtlijn volledig te testen is een source code review nodig. Er is echter niet gekozen voor een verplichte code review als onderdeel van de DigiD assessment. Observeer het gedrag van de webapplicatie op voor wat betreft onveilige uitvoer. Voer hierbij een representatieve deelwaarneming uit op de uitvoervelden van de applicatie.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken. Doelstelling: Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie	Applicatie Infrastructuur Proces	Betrokken partij(en): Applicatie-, hosting- of SAAS leverancier. Houder van de DigiD-aansluiting. Scope: De DigiD webapplicatie en webserver en bijbehorende infrastructuur. Nadere toelichting Deze norm raakt diverse aspecten van privacybevorderende en cryptografische technieken. Dit betreft de classificatie van gegevens, de encryptie van gevoelige gegevens tijdens de opslag en de encryptie van gegevens tijdens transport. Aandachtspunten hierbij zijn: de classificatie van gegevens conform de WBP door de houder van de DigiD aansluiting op basis van een risico analyse; mogelijke versleuteling of hashing van gevoelige gegevens. Het gaat hier in ieder geval om het BSN als bijzonder persoonsgegeven. Overigens geld dit alle voor gegevens die in hetzelfde DMZ worden opgeslagen als waar de webapplicatie draait. Gegevens in de backoffice vallen buiten de scope van dit onderzoek; de HTTPS configuratie en de TLS configuratie. Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer de classificatie van gegevens en daaraan gerelateerde risico analyse, de netwerkarchitectuur en het inrichtingsdocument waar de encryptie van gegevens in staat beschreven. Observeer de encryptie van gegevens. Inspecteer de HTTPS en TLS configuraties.
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen. Doelstelling: Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.	Applicatie	Betrokken partij(en): Applicatie-, hosting- of SAAS leverancier. Scope: De webserver. Nadere toelichting:

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			HTTP headers moeten de risico’s beperken van inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie. Aandachtspunten hierbij zijn: behandel alleen HTTP-requests waarvan de gegevens een correct type, lengte, formaat, tekens en patronen hebben; behandel alleen HTTP-requests van initiators met een correcte authenticatie en autorisatie; sta alleen de voor de ondersteunde webapplicaties benodigde HTTP-requestmethoden (GET, POST, etc.) toe en blokkeer de overige niet noodzakelijke HTTPrequestmethoden; verstuur alleen HTTP-headers die voor het functioneren van HTTP van belang zijn; toon in HTTP-headers alleen de hoogst noodzakelijke informatie die voor het functioneren van belang is; bij het optreden van een fout wordt de informatie in een HTTP-response tot een minimum beperkt. Een eventuele foutmelding zegt wel dat er iets is fout gegaan, maar niet hoe het is fout gegaan. Test aanpak: Observeer het gedrag van de HTTP headers en responses. Voer hierbij een representatieve deelwaarneming uit op de invoer- en uitvoermogelijkheden die de applicatie biedt.
U/PW.03	De webserver is ingericht volgens een configuratie-baseline. Doelstelling: Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.	Applicatie Infrastructuur	Betrokken partij(en): Applicatie-, hosting- of SAAS leverancier. Scope: De webserver. Nadere toelichting Deze norm richt zich enerzijds op de aanwezigheid van een configuratie-baseline voor de webserver en op de feitelijke configuratie van de webserver. Aandachtspunten hierbij zijn: directory listings worden niet ondersteund; cookie flags staan op ‘HttpOnly’ en ‘Secure’; bij alle HTTP-responses wordt de HTTP-headers ‘Content-Security-Policy: frameancestors’ en (tijdelijk) ‘X-Frame-Options’ verstuurd.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer de configuratie-baseline van de webserver. Observeer de mogelijk tot het maken van directory listings, de cookies flags en de HTTP response headers.
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen. Doelstelling: Voorkomen van misbruik van beheervoorzieningen.	Infrastructuur Proces	Betrokken partij(en): Hosting- of SAAS leverancier. Scope: De webserver en andere servers in het DMZ van de DigiD webapplicatie. Nadere toelichting: Dit betreft het gebruik van veilige netwerkprotocollen. Indien beheerinterfaces via het internet te benaderen zijn moet dit door middel van sterke authenticatie (zoals IP Sec VPN) worden afgehandeld. Er mag geen gebruik worden gemaakt van backdoors om de systemen te benaderen (ook niet voor noodtoegang). Daarnaast wordt een beknopt operationeel beleid verwacht dat o.a. de volgende: elementen bevat. Aandachtspunten voor deze norm zijn: Het gebruik van veilige protocollen (conform industriestandaarden) voor het benaderen van beheermechanismen (beheerinterfaces). Het gebruik sterke authenticatie voor zowel technisch als functioneel beheerders. Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer het operationele beleid met betrekking tot het gebruik van beheervoorzieningen en de daarbij vereiste authenticatie. Observeer de protocollen die kunnen worden gebruikt voor het benaderen van beheerinterfaces en de authenticatiemethoden die daarbij worden afgedwongen, Inspecteer de configuratie ten aanzien van de wachtwoordvereisten van de webserver en voor een deelwaarneming van minimaal één van de andere servers in het DMZ.
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar.	Infrastructuur Proces	Betrokken partij(en): Hosting- of SAAS leverancier.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
	Doelstellingen: Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.		Scope: De webserver en andere servers in het DMZ van de DigiD webapplicatie. Nadere toelichting: Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar. Hierbij kan worden verwezen naar actuele hardeningsrichtlijnen van de leverancier(s)/SANS/NIST/CIS met een vermelding van “pas toe of leg uit”. Hierbij spelen de geïdentificeerde risico’s in de “pas toe of leg uit” afweging een bepalende rol. Het gaat echter niet alleen om de hardeningsrichtlijn zelf, maar ook om het concreet toepassen ervan. De hardening van de DigiD omgeving dient stringent te zijn geregeld: alles wat open staat moet een reden hebben en alles wat open staat moet secure worden aangeboden. De hardening van interne systemen mag minder stringent. Wel moeten de beheer functies secure zijn en mogen er geen onveilige protocollen worden gebruikt, moeten standaard wachtwoorden zijn gewijzigd. Voorbeeld applicaties moeten zijn verwijderd als deze niet daadwerkelijk worden gebruikt. Aandachtspunten hierbij zijn: Inrichting van ICT-componenten (aantoonbaar) volgens de instructies en procedures van de leverancier. Bijhouden van een actueel overzicht bij van de noodzakelijke protocollen, services en accounts voor de op het platform geïnstalleerde applicaties. Deactiveren of verwijderen van alle protocollen, services en accounts op het platform als die niet volgens het ontwerp noodzakelijk zijn. Periodiek toetsen of de in productie zijnde ICT-componenten niet meer dan de vanuit het ontwerp noodzakelijke functies bieden (statusopname). Afwijkingen worden hersteld. Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer de architectuur en hardeningsstandaarden. Inspecteer de configuratiebestanden en de uitkomsten van de penetratietest.
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.	Infrastructuur	Betrokken partij(en): Hosting- of SAAS leverancier.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
	Doelstelling: Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.		Scope: Het DMZ van de DigiD webapplicatie. Nadere toelichting: DMZ en compartimentering d.m.v. (2 virtuele) firewalls. Deze eis zowel materieel (feitelijk bestaan en inrichting van DMZ) als formeel qua opzet (netwerkschema of tekening) beoordelen, eventueel op basis van een adequate beschrijving. Overigens zal de organisatie moeten aantonen dat zij voldoende inzicht heeft in de architectuur, zowel van het DMZ als van de systemen die zich daarin bevinden. Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer het netwerkarchitectuur schema inclusief de toegestane verkeersstromen tussen netwerksegmenten. Inspectie van configuratie files, firewall regels en de uitkomsten van de penetratietest.
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen. Doelstelling: Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	Infrastructuur	Betrokken partij(en): Hosting- of SAAS leverancier. Scope: Het DMZ van de DigiD webapplicatie. Nadere toelichting Beveiligingsrichtlijnen NW.04, C.06 en C.07 hangen nauw met elkaar samen: - NW.04 richt zich op de implementatie en het gebruik van IDS/IPS - C.06 richt zich op het tijdig signaleren van aanvallen - C.07 richt zich op periodieke analyse van de logging. Inkomend en uitgaand verkeer moet worden gemonitord om mogelijke aanvallen tijdig te detecteren en hier acties op te kunnen ondernemen. Hiervoor zal de organisatie een Intrusion Detection Systeem (IDS) moeten implementeren. Overigens heeft het de voorkeur om gebruik te maken van een Intrusion Prevention Systeem (IPS) dat automatisch preventieve maatregelen neemt tegen bedreigingen of een gecombineerde IDS/IPS. Ook wordt aanbevolen om het IDS of IPS te plaatsen na decryptie van het oorspronkelijk versleuteld

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			netwerkverkeer omdat anders de inhoud van de berichten niet kan worden beoordeeld door het systeem. Aandachtpunten hierbij zijn: Het gebruik van een IDS of IPS waarmee netwerkverkeer naar / van het DMZ van de DigiD webapplicatie wordt gemonitord. Een inrichtingsdocument en een beheerprocedure waarin is vastgelegd waar en hoe de IDS / IPS ingezet. Het gebruik van een adequate ruleset (b.v. Snort, Suricata, ETPro, etc.) die periodiek (= minimaal wekelijks) wordt geactualiseerd. Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer het netwerkarchitectuur schema, de inrichtingsdocumentatie en de beheerprocedure van de IDS/IPS. Inspecteer de configuratiefiles van het IDS/IPS en de signature datum van de regelset.
U/NW.05	Binnen de productieomgeving zijn beheer en productieverkeer van elkaar afgeschermd. Doelstelling: Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	Infrastructuur Proces	Betrokken partij(en): Hosting- of SAAS leverancier. Scope: Het netwerksegment met de webservers die een koppeling hebben met de DigiD omgeving van Logius inclusief de toegang vanuit internet. Nadere toelichting: Door middel van fysieke scheiding, veilige VPN verbindingen (zoals IPSec) of VLANs is het beheer- en productieverkeer van elkaar gescheiden. Deze beveiligingsrichtlijn is nauw verbonden met U/PW.05 omdat de voor het beheer uitsluitend veilige netwerkprotocollen mogen worden gebruikt. Er is een inrichtingsdocument waaruit blijkt op welke wijze content beheer (web- en database-content), applicatiebeheer en technisch beheer worden uitgeoefend. Het gebruik van fysieke scheiding, veilige VPN verbindingen (zoals IPSec) of VLANs het beheer- en productieverkeer van elkaar gescheiden. Test aanpak: Interview de verantwoordelijke functionarissen.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			Inspecteer het netwerkarchitectuurschema inclusief de toegestane verkeersstromen tussen netwerksegmenten. Inspecteer de configuratie files, firewall regels en de uitkomsten van de penetratietest.
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar. Doelstelling Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	Infrastructuur Proces	Betrokken partij(en): Hosting- of SAAS leverancier. Scope: De webserver en andere servers in het DMZ van de DigiD webapplicatie. Nadere toelichting: Voor het configureren van netwerkcomponenten is een hardeningrichtlijn beschikbaar. Hierbij kan worden verwezen naar actuele hardeningrichtlijnen van de leverancier(s)/SANS/NIST/CIS met een vermelding van “pas toe of leg uit”. Hierbij spelen de geïdentificeerde risico’s in de “pas toe of leg uit” afweging een bepalende rol. Het gaat echter niet alleen om de hardeningrichtlijn zelf, maar ook om het concreet toepassen ervan. De hardening van de DigiD omgeving dient stringent te zijn geregeld: alles wat open staat moet een reden hebben en alles wat open staat moet secure worden aangeboden. De hardening van interne systemen mag minder stringent. Wel moeten de beheer functies secure zijn en mogen er geen onveilige protocollen worden gebruikt, moeten standaard wachtwoorden zijn gewijzigd. Voorbeeld applicaties moeten zijn verwijderd als deze niet daadwerkelijk worden gebruikt. Door de vitale rol die het Domain Name System speelt in het bereikbaar houden van webapplicaties, verdient de beveiliging van DNS-services extra aandacht. Onder deze beveiligingsrichtlijn valt dan ook het verplicht gebruik van DNSSEC (DNS Security Extensions) voor de URL van het object van onderzoek. Met DNSSEC wordt de authenticiteit van DNS-antwoorden geverifieerd om misbruik te voorkomen. Aandachtspunten hierbij zijn: Bijhouden van een actueel overzicht van de noodzakelijke netwerkprotocollen, -poorten en -services. Uitschakel op de netwerkcomponenten alle netwerkprotocollen, -poorten en -services uit, behalve de noodzakelijke. Aanpassen de (beveiligings)configuraties van netwerkprotocollen, -poorten en -services op de netwerkcomponenten aan conform richtlijnen.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer de netwerkarchitectuur schema en hardeningrichtlijnen. Inspecteer de configuratiebestanden en de uitkomsten van de penetratietest.
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope). Doelstelling: Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de webapplicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	Infrastructuur Proces	Betrokken partij(en): Hosting- of SAAS leverancier. Scope: De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting: Deze netwerk based scan dient zich ten minste gericht te hebben op de hardening en patching van de infrastructuur en het detecteren van mogelijke kwetsbaarheden op de infrastructuur. Vulnerability assessments vinden intern plaats minimaal een keer per jaar en vaker op basis van een risicoafweging. De scope van het vulnerability assessment omvat ten minste de infrastructuur voor het netwerksegment met de DigiD webapplicatie. Naar aanleiding van de resultaten van de vulnerability assessment is een actieplan opgesteld om de tekortkomingen op te heffen. Er is voldoende voortgang geboekt in het opvolgen van bevindingen gezien de aard en complexiteit van de bevindingen. Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer het netwerkarchitectuur schema en de opdracht tot het uitvoeren van vulnerability assessment. Inspecteer het vulnerability assessment rapport, het actieplan naar aanleiding van de vulnerability assessment en het statusrapport met betrekking tot de bevindingen.
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	Applicatie Infrastructuur Proces	Betrokken partij(en): Applicatie-, hosting- of SAAS leverancier.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
	Doelstelling: Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).		Scope: De DigiD webapplicatie, de webserver en andere servers in het DMZ van de DigiD webapplicatie. Nadere toelichting: De voorkeur heeft het op basis van een risicoafweging enkele keren per jaar een penetratietest te laten uitvoeren, zodat ingespeeld kan worden op nieuwe bedreigingen. De penetratietest dient minimaal eenmaal per jaar te worden uitgevoerd en na significante wijzigingen. De scope van de penetratietest omvat ten minste de infrastructuur voor het netwerksegment met de DigiD webapplicatie. Naar aanleiding van de resultaten van de penetratietest is een actieplan opgesteld om de tekortkomingen op te heffen. Er is voldoende voortgang geboekt in het opvolgen van bevindingen gezien de aard en complexiteit van de bevindingen. Testaanpak: Interview de verantwoordelijke functionarissen. Inspecteer het netwerkarchitectuur schema en de opdracht tot het uitvoeren van de penetratie test. Inspecteer het penetratietest rapport, het actieplan naar aanleiding van de penetratietest en het statusrapport met betrekking tot de bevindingen.
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. Doelstelling: Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	Infrastructuur Proces	Betrokken partij(en): Hosting- of SAAS leverancier. Scope: De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting Hoewel deze richtlijn een brede reikwijdte heeft, is zij - in overleg met Logius - ingeperkt tot het detecteren van aanvallen met detectiesystemen in de webapplicatie-infrastructuur. Beveiligingsrichtlijnen NW.04, C.06 en C.07 hangen nauw met elkaar samen:

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			- NW.04 richt zich op de implementatie en het gebruik van IDS/IPS - C.06 richt zich op het tijdig signaleren van aanvallen - C.07 richt zich op periodieke analyse van de logging. Aandachtspunten bij C.06 zijn: Het definiëren van alarm situaties en drempelwaarden. Het configureren van de alarm situaties en drempelwaarden in het IDS/IPS en het genereren van de bijbehorende alerts. De inbedding van alert afhandeling in het incidentenbeheerproces inclusief escalatieprocedure. Test aanpak: Interview de verantwoordelijke functionarissen. Inspectie van de Use Cases en drempelwaarden. Inspectie van alerts en de opvolging daarvan.
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICTsystemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd. Doelstelling: Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.	Infrastructuur Proces	Betrokken partij(en): Hosting- of SAAS leverancier. Scope: De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting Beveiligingsrichtlijnen NW.04, C.06 en C.07 hangen nauw met elkaar samen: - NW.04 richt zich op de implementatie en het gebruik van IDS/IPS; - C.06 richt zich op het tijdig signaleren van aanvallen; - C.07 richt zich op periodieke analyse van de logging. De logging- en detectie-informatie en de conditie van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd. Aandachtpunten hierbij zijn: Procedurebeschrijving met daarin beschreven hoe en wanneer controles op logging moeten plaatsvinden en hoe taken op dit gebied belegd zijn. Het uitvoeren van periodieke controles op: wijzigingen aan de configuratie van webapplicaties;

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			optreden van verdachte gebeurtenissen en eventuele schendingen van de beveiligingseisen; ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden; toegangslogs. Periodieke analyse op ongebruikelijke situaties (incidenten) die de werking van webapplicaties kunnen beïnvloeden. Periodiek rapportage van de geanalyseerde en beoordeelde gelogde gegevens aan de systeemeigenaren en/of aan het management. Opvolging van bevindingen naar aanleiding van de analyse. Test aanpak: Interview de verantwoordelijke functionarissen. Inspectie van de procedurebeschrijving met betrekking tot de logging. Inspectie van de vastlegging van de periodiek review van de logging, periodieke rapportage aan het management en follow-up acties naar aanleiding van review en analyse van de logging.
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd. Doelstelling: Zeker stellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.	Applicatie Infrastructuur Proces	Betrokken partij(en): Applicatie-, hosting- of SAAS leverancier. Houder van DigiD aansluiting. Scope: De DigiD webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting: De focus ligt op het vaststellen dat het proces wijzigingsbeheer zodanig is opgezet en geïmplementeerd dat alle wijzigingen altijd eerst worden getest voordat deze in productie worden genomen en via wijzigingsbeheer worden doorgevoerd. In sommige gevallen kunnen formulieren worden gebouwd die beveiligingsrisico's introduceren en valt wijzigingenbeheer met betrekking tot formulieren wel in scope van de DigiD-assessment. Is dit niet het geval dan valt wijzigingenbeheer met betrekking tot formulieren niet in scope. Welke specifieke situatie zich voordoet hangt af van de applicatie (formulierengenerator) en de wijze waarop deze wordt gebruikt. Het is aan de auditor om te bepalen of er aanleiding is om wijzigingenbeheer ten aanzien van de formulieren in de DigiD-scope op te nemen.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			Ingeval van SAAS-toepassingen ligt de verantwoordelijkheid voor het testen van wijzigingen aan de applicatie doorgaans bij de leverancier en/of gebruikersgroep. Aandachtspunten hierbij zijn: Wijzigingsbeheer procedure, waarbij zo nodig onderscheid wordt gemaakt tussen wijzigingen op de applicatie, de servers en de netwerkcomponenten. Het inrichten van een OTAP omgeving zodat wijzigingen eerst in een testomgeving worden getest voordat zij in productie kunnen worden genomen (n.b. voor netwerk wijzigingen is een testomgeving vaak niet mogelijk). Het hanteren van een testscript en de vastlegging van de testresultaten. Een formele acceptatie voor het in productie nemen van de wijziging. Het beperken van het aantal personen die wijzigingen in productie kunnen nemen. Bij het uitbrengen van een nieuwe release van de applicatie of een grote upgrade van het onderliggende platform moet, bij voorkeur door middel van een penetratietest, worden onderzocht of er geen nieuwe kwetsbaarheden zijn geïntroduceerd. Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer de wijzigingsprocedure en de inrichting van de OTAP omgeving. Inspecteer, voor elk type wijziging (applicatie, servers, netwerk), één wijziging en de daaraan gerelateerde documentatie.
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen. Doelstelling: Zeker stellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	Applicatie Infrastructuur Proces	Betrokken partij(en): Hosting- of SAAS leverancier. Scope: Hypervisor (VM Ware, etc.). Operating system (Windows, etc.). Databases. Netwerk componenten. Firewall. Nadere toelichting: De focus is op het patching proces. Dit proces kan gedifferentieerd zijn naar bijvoorbeeld het OS, DBMS en netwerk. Applicaties en systemen dienen periodiek

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			gepatcht te worden. Een maandelijks patching cyclus is aanvaardbaar tenzij er security alerts zijn. Voor internet facing systemen dienen de laatste stabiele beveiligingspatches te zijn geïnstalleerd. Indien patching niet mogelijk is in verband met een legacy applicatie die niet meer zou functioneren na patching, zal dit risico aantoonbaar moeten zijn afgewogen. Aandachtpunten hierbij zijn: Het beschrijven van patchmanagementbeleid waarin is aangegeven hoe de organisatie omgaat met updates: hoe snel implementeert de organisatie een kritieke patch en welke stadia moet de patch doorlopen. Registratie van patches met vastlegging of de patches niet, wel of versneld worden doorgevoerd. Het tijdig doorvoeren van patches. Test aanpak: Interview de verantwoordelijke functionarissen. Inspectie van het patchmanagementbeleid. Inspectie van configuratie files en de uitkomsten van de penetratietest.

Bijlage 2 Procesmatige kwaliteitsaspecten bij DigiD penetratietesten

Van toepassing op norm C.04:

Beveiligingsrichtlijn C.04:

Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).

Doelstelling

Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).

Kwaliteitsaspecten:

Randvoorwaarden

- Penetratietester staat onafhankelijk ten opzichte van het te onderzoeken object.
- Penetratietester heeft aantoonbare eerdere ervaringen van de penetratietester met DigiD penetratietesten.
- Overeengekomen opdracht met doel, vraagstelling, normen, scope, stappenplan, doorlooptijd en budget.
- Penetratietest vrijwaring ondertekend door opdrachtgever en evt. betrokken derden zoals hosting partij.
- Afspraak over beschikbaarheid van penetratietesters en beheerders bij de onderzochte organisatie.
- Afspraak tussen auditor en penetratietester over het gebruik van penetratietesttools.
- Gedocumenteerde afspraken over communicatie tussen penetratietesters en contactpersonen bij de opdrachtgevende organisatie.
- Instemming opdrachtgever met uit te voeren penetratietest.

Scope en normstelling

- Vastgesteld object (versienummer) van het onderzoek relevant voor DigiD.
- Vastgestelde Logius normen voor DigiD (subset uit de NCSC normen), minimaal OWASP top 10, eventueel aangevuld met SANS 25, WASC criteria, GHDB en leveranciers-specifieke normen en baselines.
- Voor DigiD audit is een black box/grey box benadering, waarbij zonder veel voorkennis ingelogd wordt als gebruiker, voldoende.
- Vaststellen met welke functionele scope de volledige technische oplossing wordt afgedekt (bijvoorbeeld een selectie van formulieren waarmee alle componenten worden geraakt), waarbij wordt aangetoond dat de technische oplossing adequaat wordt getest).
- Maatwerk formulieren die niet op basis van standaard configuratie functionaliteit zijn ontwikkeld altijd testen.
- Indien standaard formulieren worden gebruikt, waarbij alleen functionele aanpassingen doorgevoerd kunnen worden, kan volstaan worden met vaststellen van de betrouwbare werking van de formulierengenerator (o.b.v. het assurance-rapport (de TPM) van de service provider).

Verkenningsfase (vaststellen ingang criteria)

- Inventarisatie gebruikte (webfacing) infrastructuur, applicaties, componenten, e.d.
- Infrastructuurtest vindt altijd plaats op de productieomgeving.
- Applicatietest vindt plaats op test omgeving. Opdrachtgever toont aan dat de versie van de applicatie van acceptatieomgeving gelijk is aan die in de productie omgeving.
- Acceptatieomgevingen met representatieve testgegevens zijn beschikbaar.
- DigiD testaccounts zijn beschikbaar en gekoppeld aan testgegevens, evt. gekoppeld aan mobiele nummers penetratietesters.
- Penetratietester(s) zijn bekend met de werking van de applicatie.
- Contactpersonen bij de opdrachtgever zijn bekend met de werking van de applicatie.

Initiële kwetsbaarheden analyse

- Fingerprinting van het object: vaststellen gebruikte merken en versies.
- Inventariseren bekende kwetsbaarheden op basis van publicaties van leveranciers en openbare cyber security bronnen.
- Selectie van tests voor aantonen van de mogelijke kwetsbaarheden.

Geautomatiseerde tests (dynamisch testen)

- Keuze geschikte penetratietest tools en hun dekkingsgraad van het te testen object (niet ieder penetratietest tool ondersteunt alle technologieën, denk aan AJAX, Silverlight, Java en dergelijke).
- Inzicht in het deel van de norm dat door de tool(s) wordt afgedekt en welk deel afzonderlijk zal moeten worden getest.
- Doorlopende bewaking door de penetratietester tijdens de uitvoering om schade te voorkomen, bij voorkeur automatisch afbreken van geautomatiseerde testen bij foutmeldingen waaruit een kritiek probleem blijkt.

Handmatige tests

- Adequate expertise van de penetratietester(s), eventueel aanwezige certificeringen ter onderbouwing; aantoonbare kennis/ervaring met gebruikte technologieën.
- Technische details van gecontroleerde SSL/TLS-certificaten en versleutelde verbindingen.
- Details van gecontroleerde cookies en volledige dekking tijdens de testen.
- Alle bevindingen uit de geautomatiseerde testen zijn handmatig geverifieerd.
- Op basis van bevindingen uit de geautomatiseerde testen zijn handmatige vervolgtesten uitgevoerd.
- Kwetsbaarheden in functionele flows zijn handmatig onderzocht, bijvoorbeeld manipulatie van velden bij meerstaps-formulieren.

Optioneel: Code review (statisch testen) afhankelijk van de norm

- In principe kunnen alle normen getest worden op basis van het bepalen van het gedrag van de applicatie. Bij gerede twijfel over het gedrag alsnog een code review uitvoeren.
- Dekkingsgraad van de review bepalen (steekproef, volledig, ..?)
- Aantoonbare ervaring van de penetratietester(s) met de programmeertaal en omgeving, eventueel beschikbare certificeringen ter onderbouwing.
- Bij gebruik van tools voor statische testen: dekkingsgraad ten opzichte van de norm.

Risicoanalyse op bevindingen (vaststellen uitgang criteria)

- Risicoafweging van aangetroffen afwijkingen t.o.v. de norm tegen het daadwerkelijk kunnen exploiteren.
- Risico's uitdrukken in kans X impact of erkende risicoclassificatie.
- Onderbouwen van de ernst van de aangetroffen afwijkingen.
- Geen uitspraken over risiconiveau vanuit business perspectief (beoordeling hiervan kan alleen door de opdrachtgever plaatsvinden).

Rapportage

- Conceptrapportage
    - Classificatie van de rapportage conform DigiD normen, beleid opdrachtgever en auditor en eventueel naar publieke standaarden.
    - Beschrijving object van het onderzoek: webfacing infrastructuur, servers, verbindingen.
    - Tijdstip van uitgevoerde testen.
    - Het ip-adres waarvandaan de test is uitgevoerd.
    - Indien van toepassing: overzicht van onderdelen die niet of onvoldoende getest konden worden.
    - Overzicht afwijkingen ten opzichte van de norm met bijbehorende mate van risico o.b.v. norm en na risicoanalyse.
    - Overzicht en details resultaten en afwijkingen per onderdeel uit de norm.
    - Proof of Concepts of details in rapportage waarmee de bevinding kan worden gereproduceerd.
    - Concrete aanbevelingen per bevinding.
- Afstemming met auditor (review).
    - Versleutelde, beveiligde uitwisseling met de auditor.
    - Controle op volledigheid en consistentie.
    - Controle of met de verkregen diepgang tijdens de testen de norm is afgedekt.
- Melden kritieke bevindingen aan opdrachtgever indien deze naar verwachting in een productieomgeving aanwezig zijn.
    - In overleg met de auditor melden.
    - Proof of Concept of stappen om te reproduceren.
    - Versleuteld, beveiligde uitwisseling details van de kwetsbaarheid.
- Afstemming met opdrachtgever.

  - Versleuteld, beveiligde uitwisseling met de auditor.
  - Afstemming over planning van oplossing en hertesten van bevindingen.
- Definitieve rapportage.
  - Versleutelde, beveiligde uitwisseling met de opdrachtgever.
  - Bevindingen waarvoor een hertest is uitgevoerd zijn als zodanig opgenomen in het rapport met de uitkomst van de hertest (t.b.v. traceerbaarheid).
- Archiveren rapportage.
  - Indien van toepassing: archivering in een afgeschermde omgeving met passende beveiligingsmaatregelen.

Periodiciteit

- Minimaal zal jaarlijkse, ten tijde van de DigiD audit, een penetratietest uitgevoerd moeten worden door een penetratietester die onafhankelijk is ten opzichte van het te onderzoeken object.
- Bij het uitbrengen van een nieuwe release van de applicatie of een grote upgrade van het onderliggende platform moet, bij voorkeur door middel van een penetratietest, worden onderzocht of er geen nieuwe kwetsbaarheden zijn geïntroduceerd. Deze penetratietest zou specifiek gefocust mogen zijn op wijzigingen in de applicatie of de infrastructuur en behoeft niet noodzakelijkerwijs door een penetratietester te worden uitgevoerd die onafhankelijk staat ten opzichte van het te onderzoeken object.
- Het is aan te bevelen om, op basis van en risicoafweging, frequenter penetratietesten uit te (laten) voeren, zodat ingespeeld kan worden op nieuwe bedreigingen.

Bijlage 3 Guidance bij de te onderzoeken ENSIA-normen relevant voor Suwinet

3.1 Reikwijdte verantwoording

Wij vragen in deze bijlage 3 de aandacht voor de reikwijdte en invulling van de verantwoording betreffende het gebruik van GeVSde toepassing van de voorziening Suwinet-/DKD-Inlezen en betreffende het gebruik van Suwinet voor niet-SUWI-taken. Ook Suwi inkijk functionaliteit wordt in navolgende toegelicht. Suwi inkijk betreft de zuivere raadpleeg faciliteit. Suwilezen betreft de gemeentelijke bedrijfsapplicatie waarin gegevens via Suwinet- of DKD-Inlezen kunnen worden ingelezen (= inleesapplicaties).

De Autoriteit Persoonsgegevens (AP) heeft indertijd onderzoek gedaan naar de aansluiting van niet-SUWI-partijen op Suwinet (november 2014). Bij dit onderzoek heeft de AP vastgesteld dat in een aantal overeenkomsten sprake is van toepassing van Suwinet-Inlezen. Op grond van het wettelijk kader SUWI heeft de AP geconcludeerd dat de beheerder BKWI net als bij Suwinet-Inkijk, overzicht en controle moet hebben over het feitelijk gegevensgebruik door afnemers. Deze toelichting onderstreept ook op deze criteria het belang van beveiliging.

3.2 Samenhang Inkijk, Inlezen, SUWI-taken en niet-SUWI-taken

Suwinet-Inkijk en Suwinet/DKD-Inlezen kunnen zowel bij SUWI-taken als bij niet-SUWI-taken worden toegepast. Bij suwi-taken is het dkd-inlezen geregeld via ‘Inlichtingenbureau’, bij niet-suwi is het suwi-inlezen via BKWI.

	SUWI-taken	Niet-SUWI-taken
Suwinet-Inkijk applicatie	Reikwijdte eerdere onderzoeken Inspectie SZW	Reikwijdte eerdere AP-onderzoek

Inleesapplicatie (gemeentelijke bedrijfsapplicatie waarin gegevens via Suwinet- of DKD-Inlezen worden ingelezen)		Reikwijdte eerdere AP-onderzoek[1]

Alle 3 de kwadranten zijn onderdeel van de reikwijdte van de verantwoording ENSIA (Collegeverklaring en IT-Audit) per 31 december 2017. In de bijlage 1 bij de notitie Verantwoordingsstelsel ENSIA is daarover het volgende vermeld: *"Conform het Suwinet specifieke normenkader afnemers betekent dit dat de eisen betreffende logging over het gegevensgebruik op medewerkersniveau, het opstellen van gebruiksrapportages en het op basis daarvan controleren van het gebruik op alle gemeentelijke applicaties van toepassing zijn waarin via Suwinet-Inlezen of DKD-Inlezen ingelezen gegevens worden verwerkt."*

Aanvullend op de mapping op de BIG met het verantwoordingsstelsel ENSIA betekent dit dat de criteria C05 (loggen) en C06 (controleren en bijsturen) van toepassing zijn op de Inleesapplicaties.

Voor de korte termijn heeft UWV de betreffende overeenkomsten in het onderzoek van de AP van een addendum voorzien waarin is bepaald dat jaarlijks een auditrapportage over de volgende 4 punten aan BKWI wordt verstrekt:
- Het loggen van het gebruik van gegevens in de inlezende applicatie op medewerkersniveau;
- Het opstellen van gebruiksrapportages ter controle op misbruik en oneigenlijk gebruik door medewerkers;
- Het nagaan of sprake is van misbruik of oneigenlijk gebruik van medewerkers
- verbeteracties bij misbruik en oneigenlijk gebruik worden genomen en/of sancties opgelegd.

Voor de verantwoording over 2016 zijn IT-audits naar bovenstaande punten uitgevoerd. Voor de structurele oplossing verwijst UWV naar de invoering van deze ENSIA aanpak. ENSIA is er namelijk op gericht dat alle gemeenten verantwoording afleggen en transparantie bieden over het gebruik van Suwinet-inkijk, Suwi-inlezen en DKD-Inlezen.

---

[1] Het onderzoek van de AP had betrekking op de toegang van niet-Suwi-partijen tot Suwinet. Gedurende dit onderzoek kwam de toepassing van Suwinet-Inlezen bij dergelijke aansluitingen naar voren.

Voor het aansluiten van zogenoemde niet-SUWI-partijen voorziet de Regeling SUWI in een aansluitprotocol. Via dit protocol zijn overeenkomsten tussen UWV (bron), beheerder (BKWI) en afnemers (gemeenten) op Suwinet afgesloten. In 2016 zijn deze overeenkomsten door UWV herijkt en is het auditreglement UWV toegepast. Dit reglement voorziet in een aantal beveiligingsnormen en een auditverplichting. UWV en gemeenten hebben deze overeenkomsten ondertekend. De beleidskaders GeVS zijn van toepassing en dit betekent toepassing van de Verantwoordingsrichtlijn Beveiliging & Privacy met de daarin opgenomen beveiligingsnormen.

3.3 Belangrijke feiten nog eens op een rij:

- Alle normen uit de onderstaande tabel zijn van toepassing m.b.t. tot de Suwi-inkijk faciliteit. Dit met de kanttekeningen dat bepaalde normen niet door de gemeente maar door BKWI worden ingevuld/geregeld, bijvoorbeeld wachtwoorden en logging [Ingestoken op Suwi-Inkijk worden naar verhouding relatief veel punten (automatisch) afgedwongen door BKWI]
- Voor DKD-inlezen en Suwi-inlezen zijn alleen de normen C05, C06 van toepassing. DKD-inlezen en Suwi-inlezen staan daarom alleen in de scope vermeld bij deze twee normen; De relevante vraag is daarbij of onbevoegde personen toegang hebben gehad tot de inleesapplicatie.
- Bij bestudering van gebruik van gegevens is de IT auditor met name voor logging aangewezen op de mogelijkheden van de inlezende gemeentelijke applicaties (inlees applicaties) die via een interface verbonden zijn met SUWINET.

*) Bij C06 van de tabel merken wij voor wat betreft de logging twee mogelijkheden op.

1^{e} mogelijkheid: Logging BKWI: Deze is beschikbaar voor Suwi inkijk. BKWI stelt deze logging maandelijkse beschikbaar. Daarbij wordt een onderscheid gemaakt tussen de standaardlogging en directe raadpleging van logging bij een incident. Voor eerstgenoemde wordt voorgeschreven om meer dan 1 maal per jaar de logging te analyseren. Geadviseerd wordt minimaal halfjaarlijks dan wel per kwartaal. Voor directe raadpleging dient een onafhankelijke functionaris binnen de gemeente daartoe te worden gemachtigd.

2^{e} mogelijkheid: Logging specifiek: De logging met betrekking tot inlezen betreft de logging op de inlezende applicatie(s) van de gemeente en is situationeel. Ook voor deze vorm wordt voorgeschreven om meer dan 1 maal per jaar de logging te analyseren. Geadviseerd wordt minimaal halfjaarlijks dan wel per kwartaal.

3.4 Slotopmerking

Hierna is de normering nader toegelicht. In het kader van het ENSIA-project is een matching uitgevoerd van de in de ENSIA-vragenlijst opgenomen BIG-normen met de relevante Suwinet normen. Het gaat in totaal om 13 BIG-normen waar 11 relevante Suwinet normen aan gekoppeld zijn.

Daarbij wordt nog benadrukt dat vanuit Governance-perspectief en de '*Tone-at-the-top*' de zichtbare betrokkenheid van het College van B&W bij informatiebeveiliging aangetoond dient te kunnen worden. De gemeente dient als afnemer het thema informatieveiligheid expliciet als een strategisch agendapunt te benoemen. Dit moet met name blijken uit het aantoonbaar voldoen aan (en handhaven van) de vereiste beveiligingsvoorwaarden die aan een Suwinet-aansluiting worden gesteld en vastgesteld beleid met betrekking tot de wijze waarop de uitwisseling van gegevens in dat verband plaatsvindt.

Ref	Beveiligingsrichtlijn Suwinet	Type/domein	Handreiking voor de IT auditor
ENSIA: H 5.1 Informatiebeveiligingsbeleid Suwinet: B.01 BIG: 5.1.1	Criterium: De Afnemer heeft voor de aansluiting op Suwinet expliciet aandacht besteed aan het stelsel van beveiligingsmaatregelen in zijn informatiebeveiligingsbeleid, of hiervoor een apart aansluitingsbeleid ontwikkeld. Doelstelling: Richting geven aan en handhaven van beveiliging van de Suwinet aansluiting en de gegevens die worden getransporteerd en ervoor te zorgen dat aansluiting van de organisatie op Suwinet aantoonbaar aan de vereiste beveiligingsvoorwaarden voldoet. *Risico:* *Het risico bestaat dat de bescherming van de aansluiting op Suwinet, in tegenstelling tot bescherming van haar eigen ICT omgeving, onvoldoende aandacht krijgt.*	Beleidsdomein	Betrokken partij(en): Gemeenten. Scope: Suwinet aansluitbeleid. Suwinet-Inkijk Toelichting: De gemeente moet beschikken over een aansluitbeleid op Suwinet (eventueel als onderdeel van het informatiebeveiligingsbeleid). Het aansluitbeleid betreft het beleid aangaande de bescherming van de eigen informatiehuishouding in relatie tot de eigen delen van Suwinet en de via Suwinet beschikbaar gestelde gegevens. Test aanpak: Interview de verantwoordelijke functionarissen. Inspectie van het informatiebeveiligingsbeleid/aansluitingsbeleid. Deze dient inzicht te geven in de type maatregelen voor de beveiliging van de eigen delen van Suwinet (bijv. organisatorische-, technische- en beheersingsmaatregelen). Stel tevens vast dat het beleid is vastgesteld door het College van Burgemeesters en Wethouders.
ENSIA: H 6.1: Interne organisatie Suwinet: B.04 BIG: 6.1.2	Criterium: De Afnemer heeft een Beveiligingsfunctie Suwinet (GeVS) benoemd en taken en verantwoordelijkheden vastgesteld. Doelstelling: Het voorkomen dat risico’s optreden als gevolg van het ontbreken van coördinatie op het gebied van	Beleidsdomein	Betrokken partij(en): Gemeenten. Scope: Beveiligingsfunctie Suwinet (GeVS). Suwinet-Inkijk Toelichting:

Ref	Beveiligingsrichtlijn Suwinet	Type/domein	Handreiking voor de IT auditor
	activiteiten aangaande de bescherming van de eigen delen van Suwinet. *Risico:* *Het risico bestaat dat door gebrek aan coördinatie van activiteiten niet op beveiligingsincidenten wordt geacteerd en dat door wijzigingen nieuwe kwetsbaarheden ontstaan.*		Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit de verschillende delen van de organisatie met relevante rollen en functies. Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer het informatiebeveiligingsbeleid en stel vast dat taken, bevoegdheden en verantwoordelijkheden ten aanzien van de IB functie formeel zijn vastgesteld en stel vast dat deze functie ook als zodanig is ingericht Stel vast dat een incidentmanagementproces (beveiligingsincidenten) ten aanzien van Suwinet is ingericht en stel het bestaan vast met een deelwaarneming van ten minste één. Stel vast dat beveiligingsincidenten worden geanalyseerd, gerapporteerd en waar nodig aanvullende maatregelen worden getroffen.
ENSIA: H 6.1 Interne organisatie / H 10.1 Bedieningsprocedures en-verantwoordelijken Suwinet: B.05 BIG: 6.1.3 en 10.1.3	Criterium: De aangesloten organisatie op Suwinet heeft de type-rollen onderkend, de daarbij behorende de taken en verantwoordelijkheden vastgesteld en vastgelegd en noodzakelijke functiescheiding beschreven. Doelstelling: Ervoor zorgen dat de juiste taken en verantwoordelijkheden binnen de onderkende rollen juist worden uitgevoerd met inachtneming van de juiste functiescheiding voor zover de organisatiegrootte dit toelaat. *Risico:* *Onduidelijke taken en verantwoordelijkheden en het ontbreken van juiste functiescheiding kunnen leiden tot:*	Beleidsdomein	Betrokken partij(en): Gemeenten. Scope: Taken, verantwoordelijkheden en functiescheiding. Suwinet-Inkijk Toelichting: Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd. Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. Het gaat hierbij om de verantwoordelijkheden van lijnmanagement, security management, maar ook bijvoorbeeld informatiemanagement en control.

Ref	Beveiligingsrichtlijn Suwinet	Type/domein	Handreiking voor de IT auditor
	- misbruik van bevoegdheden, *- te ruim toegekende bevoegdheden,* *- over het hoofd zien van en/of tot implementatie van tegenstrijdige beveiligingsmaatregelen.*		Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer de functie/taakbeschrijvingen van beheerders, de autorisatiematrix en het autorisatiebeheerproces, en stel vast dat deze voldoen aan bovenstaande aandachtspunten.
ENSIA: H 8.2 Tijdens het dienstverband / H 11.2 Beheer van toegangsrechten van gebruikers Suwinet: U.02 BIG: 8.2.2 en 11.2.1	Criterium: De Afnemer beheerst de toewijzing van autorisaties op basis van een formeel autorisatie beheerproces waarbij het van essentieel belang is, dat het wijzigen (ook intrekken of blokkeren) van toegangsrechten voor Suwinet tijdig wordt uitgevoerd. Doelstelling: Gebruikers en beheerders de juiste toegangsrechten geven (niet meer en niet minder) dan welke nodig zijn voor de hen opgedragen (wettelijke)taken. *Risico:* *Het risico bestaat dat medewerkers onrechtmatig toegang hebben tot Suwinet of tot de via Suwinet beschikbaar gestelde gegevens.* *Voor Suwinet geldt een verhoogd risico omdat het Suwinet account van een organisatie ook toegang tot Suwinet kan krijgen vanuit het domein van een ander op Suwinet aangesloten organisatie.*	Uitvoeringsdomein	Betrokken partij(en): Gemeenten. BKWI. Scope: Autorisatie beheerproces Suwinet-Inkijk Toelichting: Procedurebeschrijvingen die beschikbaar zijn voor registreren en afmelden van gebruikers voor enkele informatiesystemen of -diensten, kopie procedurebeschrijving voor de registratie van gebruikers en beheerders, kopie van informatie waaruit blijkt dat de organisatie gebruiker-id's conform de procedures heeft toegekend. Te denken aan: kopie van aanvraagformulieren voor gebruikers-id's, kopie uit systeem waaruit blijkt dat de gebruikers een unieke gebruikersidentificatie (ID) hebben, kopie twee meest recente rapportages waaruit blijkt dat de organisatie controle uitvoert op verwijderen of blokkeren van overtollige gebruiker-id's en accounts. Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer het autorisatiebeheerproces en stel voor joiners, movers en leavers, het bestaan vast met een deelwaarneming van ten minste één.

Ref	Beveiligingsrichtlijn Suwinet	Type/domein	Handreiking voor de IT auditor
			Inspecteer de toegekende autorisaties en de resultaten en opvolging van de periodieke review. Stel vast dat de gemeente de actualiteit van de toegangsrechten toegekend door BKWI heeft geëvalueerd.
ENSIA: H 11.2 Beheer van toegangsrechten van gebruikers / H 11.5 Toegangsbeveiliging voor besturingssystemen Suwinet: U.03 BIG: 11.2.1 en 11.5.2	Criterium Elke gebruiker/beheerder behoort over een unieke identificatiecode te beschikken (User-ID) voor uitsluitend persoonlijk gebruik, ook behoort een geschikte authenticatie techniek te worden gekozen. Doelstelling Bewerkstelligen dat de geclaimde identiteit van de gebruiker kan worden bewezen en dat daardoor alleen bevoegde gebruikers toegang krijgen tot Suwinet diensten. *Risico:* *Onbevoegde gebruikers kunnen toegang krijgen tot Suwinet diensten.*	Uitvoeringsdomein	Betrokken partij(en): Gemeenten. Scope: Toegangsmechanisme: gebruikersidentificatie-en authenticatie (IA). Suwinet-Inkijk Toelichting: Elke gebruiker/beheerder behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen. NB. BKWI bepaalt de authenticatietechniek voor Suwinet-Inkijk. Hierin heeft de gemeente geen keuze. Voor gebruikers- en beheeractiviteiten met hoog risicoprofiel dienen sterkere authenticatiemiddelen worden ingezet, Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer het autorisatiebeheerproces en stel vast dat dit proces in lijn is met bovenstaande aandachtspunten. Inspecteer het wachtwoordbeleid en de wachtwoordinstellingen en stel vast dat deze voldoen aan bovenstaande aandachtspunten.
ENSIA: H 12.3 Cryptografische beheersmaatregelen Suwinet: U.11	Criterium: De Afnemer behoort alle netwerkverbindingen waarover Suwinet gegevens worden uitgewisseld beveiligd te hebben tegen ongeautoriseerde	Uitvoeringsdomein	Betrokken partij(en): Gemeenten. Scope:

Ref	Beveiligingsrichtlijn Suwinet	Type/domein	Handreiking voor de IT auditor
BIG: 12.3.1	toegang overeenkomstig het aansluitingsbeleid Suwinet. <u>Doelstelling:</u> Het voorkomen van ongeautoriseerde toegang tot netwerkdiensten. *<u>Risico:</u>* *Ondanks het besloten karakter van Suwinet bestaat het risico dat de toegang tot gegevens niet adequaat is beschermd.*		Netwerkverbindingen. Suwinet-Inkijk <u>Toelichting:</u> Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie. <u>Test aanpak:</u> Interview de verantwoordelijke functionarissen. Inspecteer de classificatie van gegevens en daaraan gerelateerde risicoanalyse, de netwerkarchitectuur en het inrichtingsdocument waar de encryptie van gegevens in staat beschreven, en stel vast dat deze voldoen aan bovenstaande aandachtspunten. Stel vast bij welke provider de gemeente de beveiligde verbinding heeft afgenomen. NB: Een gemeente kan alleen via een beveiligde verbinding aansluiten op Suwinet. Observeer de encryptie van gegevens. Inspecteer of TLS toegepast wordt.
ENSIA: H 5.1 Informatiebeveiligingsbeleid / H 6.1 Interne organisatie Suwinet: C.01 BIG: 5.1.2 en 6.1.1	<u>Criterium:</u> (De implementatie van) het aansluitbeleid wordt periodiek beoordeeld op veranderingen in de wetgeving, wijziging van functionaliteit en uit te wisselen gegevens en veranderde technologieën. <u>Doelstelling:</u> Bewerkstellingen dat de getroffen beveiligingsmaatregelen continue voldoen aan het juiste beveiligingsniveau. *<u>Risico:</u>*	Control	<u>Betrokken partij(en):</u> Gemeenten. <u>Scope:</u> Evaluatie van aansluitbeleid. Suwi-Inkijk <u>Toelichting:</u> Het aansluitbeleid dient derhalve periodiek te worden geëvalueerd en indien nodig te worden bijgestuurd. Het hoogste management behoort actief informatiebeveiliging (middels het ISMS/P&C cyclus, MT vergaderingen etc.) binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.

Ref	Beveiligingsrichtlijn Suwinet	Type/domein	Handreiking voor de IT auditor
	De getroffen beveiligingsmaatregelen kunnen ontoereikend zijn in relatie tot aangescherpte wetgeving, verandering van risicoklasse van gegevens en de toegepaste technologieën.		Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer de verslagen van de periodieke evaluaties en de opvolging hiervan en stel vast dat deze voldoen aan bovenstaande aandachtspunten. Stel vast dat er aandacht wordt geschonken aan awareness voor informatiebeveiliging binnen de organisatie.
ENSIA: H 11.2 Beheer van toegangsrechten van gebruikers Suwinet: C.04 BIG: 11.2.4	Criterium: Het verantwoordelijke management behoort de toegangsrechten van gebruikers/beheerders tot de Suwinet diensten regelmatig te beoordelen in een formeel proces (cyclisch proces). Doelstelling: Het vaststellen of: de autorisaties en veranderingen hierin juist en tijdig zijn aangebracht, de juiste functiescheiding zijn toegepast en voldaan wordt aan de principes van doelbinding en proportionaliteit, oneigenlijk autorisatie-toekenningen hebben plaatsgevonden. *Risico:* *Bij het ontbreken van controle op de toegangsrechten worden afwijkingen in het autorisatieproces niet gesignaleerd worden.* *Bij het ontbreken controles op het gebruik van autorisaties wordt misbruik niet gesignaleerd.*	Control	Betrokken partij(en): Gemeenten. Scope: Beoordeling van toegangsrechten. Suwinet-Inkijk Toelichting: Het (lijn)management behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces. Het management beoordeelt of: de autorisaties en veranderingen hierin juist en tijdig zijn aangebracht, de juiste functiescheiding zijn toegepast en voldaan wordt aan de principes van doelbinding en proportionaliteit, oneigenlijk autorisatie-toekenningen hebben plaatsgevonden. Testaanpak: Interview de verantwoordelijke functionarissen. Inspecteer de autorisatiematrix, de toegekende autorisaties en de resultaten en opvolging van de periodieke review en stel vast dat deze voldoen aan bovenstaande aandachtspunten. Inspecteer de management reviews.
ENSIA: H 10.10 Controle Suwinet C.05	Criterium: Activiteiten van gebruiker en beheerders, uitzonderingen en informatiegebeurtenissen behoren te	Control	Betrokken partij(en): Gemeenten.

Ref	Beveiligingsrichtlijn Suwinet	Type/domein	Handreiking voor de IT auditor
BIR: 10.10.1	worden vastgelegd in audit-logbestanden en te worden bewaard, ten behoeve van controles. Doelstelling: Alle handelingen die betrekking hebben op gebruikers en beheerders moeten herleidbaar zijn naar individuele personen. *Risico:* *Zonder vastlegging en bewaking kan achteraf niet worden vastgesteld wie bepaalde handelingen heeft uitgevoerd.*		Scope: Gebruik logging (zie C.06) Suwinet inkijk (logging door BKWI) Suwinet inlezen (logging door gemeente) DKD-Inlezen (logging door gemeente) Toelichting: Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole. De relevante vraag is daarbij of onbevoegde personen toegang hebben gehad tot de inleesapplicatie. Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer de procedurebeschrijving met betrekking tot de logging en stel vast dat deze voldoet aan bovenstaande aandachtspunten. Inspectie van de locatie van de logbestanden.
ENSIA: H 10.10 Controle Suwinet C.06 BIG: 10.10.1 en 10.10.2	Criterium: De log-informatie (zie toelichting *) wordt regelmatig gemonitord (signaleren, analyseren rapporteren en bijsturen) Doelstelling: Bewerkstellingen dat tijdig correctieve maatregelen kunnen worden getroffen en informatie te kunnen verschaffen over activiteiten van gebruikers en beheerders van de Suwinet diensten en	Control	Betrokken partij(en): Gemeenten. Scope: Monitoring en rapportage. Suwinet-Inkijk/Suwinet-Inlezen /DKD-Inlezen. Toelichting: Er behoren procedures te worden vastgesteld om het gebruik van ICT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.

Ref	Beveiligingsrichtlijn Suwinet	Type/domein	Handreiking voor de IT auditor
	vaststellen of oneigenlijk gebruik of misbruik is gemaakt van autorisatie. Risico: *Afwijkingen niet worden gesignaleerd en derhalve niet kunnen worden aangepakt.*		Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer de procedurebeschrijving met betrekking tot het monitoren van de logging en stel vast dat deze voldoet aan bovenstaande aandachtspunten. Inspectie van de vastlegging van de periodiek review van de logging, periodieke rapportage aan het management en follow-up acties naar aanleiding van review en analyse van de logging.
ENSIA: H 10.10 Controle Suwinet: C0.7 BIG: 10.10.2	Criterium: De Afnemer voert periodiek evaluaties op de technische en organisatorische beoordelingsrapportages en neemt noodzakelijke verbeteracties. Doelstelling: Bewerkstelligen dat zich geen leemtes in de beveiliging van IAA (Identificatie, Authenticatie en Autorisatie) mechanismen voordoen. *Risico:* *Zonder evaluaties van beide type rapportages bestaat het risico dat IAA mechanismen niet ingericht zijn conform de beveiligingseisen en dat zich afwijkingen en of bedreigingen hebben voorgedaan waartegen maatregelen moeten worden getroffen.*	Control	Betrokken partij(en): Gemeenten. Scope: Evaluatie van IAA rapportages. Suwinet-Inkijk/Suwinet-Inlezen Toelichting: Er behoren procedures te worden vastgesteld om het gebruik van ICT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld. Test aanpak: Interview de verantwoordelijke functionarissen. Inspecteer de periodieke rapportage van de systeem-verantwoordelijke aan het management en follow-up acties naar aanleiding hiervan, en stel vast dat deze voldoet aan bovenstaande aandachtspunten.

Tabel SUWI

Bijlage 4 Collegeverklaring

Het college van burgemeester en wethouders van de gemeente <naam gemeente> legt met deze verklaring verantwoording af over geselecteerde informatiebeveiligingsnormen inzake DigiD en Suwinet op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

Het doel van ENSIA is om verantwoording over informatieveiligheid af te leggen aan de gemeenteraad. ENSIA sluit aan op de gemeentelijke planning en controlcyclus voor informatiebeveiliging, neemt de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie. Hierdoor heeft het gemeentebestuur meer overzicht over de informatiebeveiliging van de gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad en andere belanghebbenden.

Zo structureert ENSIA ook de verticale verantwoording van gemeenten richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Reikwijdte verklaring

Deze verklaring betreft de onderdelen van de ENSIA systematiek waarover assurance wordt gevraagd van een onafhankelijke IT-auditor. Voor het jaar 2017 betreft dit DigID (aansluitnummers <aansluitnummers >) en Suwinet. De verklaring omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0, op het openbare deel van de websites van het ministerie van BZK[1]) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI[2] en bijlage 1 van de notitie verantwoordingsstelsel op website ENSIA[3] voor de selectie van normen). De normen vinden hun basis in internationale standaarden en zijn geschikt voor het doel van deze collegeverklaring. De collegeverklaring omvat niet de werking van de maatregelen over 2017.

<Alleen bij uitbesteding van DigiD beheersmaatregelen: De beheersingsmaatregelen inzake DigiD die zijn uitbesteed vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring “bijlage 1 DigiD” blijkt over welke beheersmaatregelen en DigiD-normen door de dienstverlener aan wie de beheersmaatregelen zijn uitbesteed verantwoording wordt afgelegd. Deze collegeverklaring en de verantwoording van de dienstverlener dekken tezamen de geselecteerde normen inzake DigiD af. >

<Alleen bij gebruik Suwinet in samenwerkingsverbanden: De beheersingsmaatregelen rond het gebruik van Suwinet die belegd zijn bij <de samenwerkingsverbanden> vallen onder de reikwijdte van deze collegeverklaring.>

Deze collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De departementen en de gemeenteraad die toezien op de veiligheid van DigiD en Suwinet zijn via bij deze collegeverklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk …) en Suwinet (bijlage 2 Suwinet met kenmerk…) geïnformeerd over de afwijkingen van de normen.

Verklaring college

Het college verklaart dat bij gemeente <naam gemeente> op 31 december 2017 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigID en Suwinet. <Alleen bij uitzonderingen: voor Suwinet en/of de DigiD–aansluitnummers <aansluitnummers >wordt niet aan alle geselecteerde normen voldaan>.

De op de uitzonderingen gerichte beheersmaatregelen zijn in verbeterplannen opgenomen, zijn belegd en worden gemonitord.

[Plaats, datum]

[College gemeente]

1 https://www.logius.nl/ondersteuning/digid/beveiligingsassessments/normenkader-v20-voor-2017/
2 https://www.bkwi.nl/nieuws/nieuw-normenkader-voor-gemeenten
3 https://www.ensia.nl/

Bijlage 5 Assurance-rapport

Assurance-rapport van de onafhankelijke IT-auditor

Aan: Opdrachtgever

Ons oordeel <Bij bevindingen: 'Ons oordeel met beperking', 'Ons afkeurend oordeel', etc.>

Wij hebben de bijgevoegde Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging van DigiD en Suwinet (inclusief bijlage 1 DigiD en bijlage2 Suwinet waarnaar in de collegeverklaring wordt verwezen) van gemeente <naam gemeente> onderzocht.

Naar ons oordeel is bijgevoegde Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging van DigiD en Suwinet (inclusief bijlage 1 DigiD en bijlage 2 Suwinet waarnaar in de collegeverklaring wordt verwezen) van gemeente <naam gemeente> in alle van materieel belang zijnde aspecten, juist.

De Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging van DigiD en Suwinet (hierna Collegeverklaring ENSIA 2017) omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0, op het openbare deel van de websites van het ministerie van BZK) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI en bijlage 1 van de notitie verantwoordingsstelsel op website ENSIA voor de selectie van normen). Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel omtrent DigiD en Suwinet. De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel staan beschreven in de collegeverklaring.

<Alleen bij bevindingen: een passage met paragraafkop 'Onderbouwing van ons oordeel met beperking' over beperkingen bij het onderzoek. Zoals in de Collegeverklaring ENSIA 2017 is aangegeven wordt nog niet aan alle normen inzake DigiD en/of Suwinet voldaan. Plus nadere uiteenzetting van de normen en waarom hier nog niet aan is voldaan e.e.a. zoals ook vermeld in de Collegeverklaring. Zo'n uiteenzetting is geen generieke verwijzing naar de bijlagen waar per norm een conclusie is getrokken, maar een expliciete opsomming van de normen en waarom hier nog niet aan is voldaan>.

Benadrukking aangelegenheden

<Alleen bij uitbesteding van DigiD beheersingsmaatregelen: de beheersingsmaatregelen inzake DigiD die zijn uitbesteed vallen buiten de reikwijdte van de collegeverklaring en dit assurance-rapport. Wij hebben wel vastgesteld dat onze assurance bij deze collegeverklaring

en de assurance bij de verantwoording van de dienstverlener aan wie de beheersingsmaatregelen zijn uitbesteed tezamen de geselecteerde normen inzake DigiD afdekken.

In de collegeverklaring is vermeld dat op de uitzonderingen gerichte beheersingsmaatregelen in verbeterplannen zijn opgenomen, zijn belegd en worden gemonitord. Ons onderzoek heeft zich niet gericht op deze verbeterplannen en het beleggen en monitoring hiervan.

Deze aanvullende informatie is niet bedoeld om afbreuk te doen aan ons oordeel.

De basis voor ons oordeel < Bij bevindingen aan te passen in: Basis voor ons oordeel met beperkingen, etc.>

Wij hebben onze assurance-opdracht met betrekking tot de Collegeverklaring ENSIA 2017 uitgevoerd volgens Nederlands recht, waaronder de Richtlijn 3000 (Herzien) ‘Assuranceopdrachten door IT-auditors’ van NOREA. Deze assurance-opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Onze verantwoordelijkheden voor de assurance-opdracht betreffende de Collegeverklaring ENSIA 2017’.

Wij hebben de vereisten van het Reglement Gedragscode (‘Code of Ethics’) van NOREA nageleefd, welke is gebaseerd op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

Wij vinden dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor ons oordeel.

Beperking in gebruik en verspreidingskring

Dit assurance-rapport is bestemd voor gebruikers van de Collegeverklaring ENSIA 2017. De Collegeverklaring ENSIA 2017 is opgesteld voor de gemeenteraad en voor de departementen die toezien op de veiligheid van DigiD en Suwinet. Doel van de Collegeverklaring ENSIA 2017 is om de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet te informeren over het in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigiD en Suwinet. Ons assurance-rapport is derhalve uitsluitend bestemd voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet en dient niet te worden verspreid aan of te worden gebruikt door anderen.

Beperkingen van interne beheersingsmaatregelen

Interne beheersingsmaatregelen kunnen vanwege hun aard niet alle fouten of omissies bij het verwerken of rapporteren van transacties voorkomen of ontdekken.

Werking niet onderzocht

Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen en brengen daarover geen oordeel tot uitdrukking.

Verantwoordelijkheden van het college van gemeente <naam gemeente>

Het college van burgemeester en wethouders van gemeente <naam gemeente> is verantwoordelijk voor het opstellen van de Collegeverklaring ENSIA 2017. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet dienen voldoende inzicht te hebben om deze collegeverklaring, samen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die zelf worden uitgevoerd, te beschouwen wanneer zij de risico's van afwijkingen van materieel belang in relatie tot DigiD en Suwinet inschatten.

De criteria waarvan bij het maken van deze verklaring gebruik werd gemaakt hielden in dat:

- De risico's die het bereiken van de geselecteerde normen DigiD en Suwinet in gevaar brengen, werden geïdentificeerd;
- De onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de vermelde interne beheersingsdoelstellingen niet zouden verhinderen.
- Het college ook verantwoordelijk is voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de collegeverklaring ENSIA 2017 mogelijk te maken zonder afwijkingen van materieel belang als gevolg van fraude of fouten.

Onze verantwoordelijkheden voor de assurance-opdracht betreffende de collegeverklaring ENSIA 2017

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van een assurance-opdracht dat wij daarmee, met een redelijke mate van zekerheid voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel. Een redelijke mate van zekerheid wil zeggen dat onze assurance-opdracht is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens onze assurance-opdracht niet alle materiële fouten en fraude ontdekken.

Wij passen het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van de ethische voorschriften, professionele standaarden en andere wet- en regelgeving.

Afwijkingen kunnen ontstaan als gevolg van fraude of fouten en zijn materieel indien redelijkerwijs kan worden verwacht dat deze, afzonderlijk of gezamenlijk, van invloed kunnen zijn op de beslissingen die gebruikers op basis van de Collegeverklaring ENSIA 2017 nemen. De materialiteit beïnvloedt de aard, timing en omvang van onze assurance-werkzaamheden en de evaluatie van het effect van onderkende afwijkingen op ons oordeel.

Wij hebben deze assurance-opdracht professioneel kritisch uitgevoerd en hebben waar relevant professionele oordeelsvorming toegepast in overeenstemming met de Richtlijn 3000 (Herzien) ‘Assuranceopdrachten door IT-auditors’ van NOREA.

Onze assurance-opdracht bestond onder andere uit:

- het verkrijgen van kennis omtrent de Collegeverklaring ENSIA 2017 en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen. Deze werkzaamheden hebben niet als doel om een oordeel uit te spreken over de effectiviteit van de interne beheersing van de gemeente;
- het op basis van deze kennis inschatten van de risico's dat de Collegeverklaring ENSIA 2017 onjuistheden van materieel belang bevat als gevolg van fraude en fouten, het in reactie op deze risico’s bepalen en uitvoeren van assurance-werkzaamheden en het verkrijgen van assurance-informatie die voldoende en geschikt is als basis voor ons oordeel. Bij fraude is het risico dat een afwijking van materieel belang niet ontdekt wordt groter dan bij fouten. Bij fraude kan sprake zijn van samenspanning, valsheid in geschrifte, het opzettelijk nalaten transacties vast te leggen, het opzettelijk verkeerd voorstellen van zaken of het doorbreken van de interne beheersing;
- het reageren op de ingeschatte risico's, waaronder het ontwikkelen van een algehele aanpak, en het bepalen van de aard, de tijdsfasering en de omvang van verdere procedures;
- het uitvoeren van verdere procedures die duidelijk zijn gekoppeld aan de gesignaleerde risico's, waarbij gebruik wordt gemaakt van een combinatie van inspectie, waarnemingen ter plaatse en inwinnen van inlichtingen; en
- het evalueren van de toereikendheid van de assurance-informatie.

Plaats en datum

... (naam IT-auditeenheid)

... (naam IT-auditor RE)

Bijlage 6 Overwegingen Audit in samenwerkingsverbanden Suwinet

De uitgangspunten

Het nieuwe normenkader voor afnemers is geïntegreerd in de BIG uitvraag van ENSIA. Waar dat niet kan zijn beperkt Suwi-specifieke normen in de vragenlijst opgenomen. De gemeente geeft in de collegeverklaring aan in hoeverre wordt voldaan aan een subset van dit normenkader. Suwi-regelgeving vraagt van gemeentebestuur een door een RE afgegeven assurance op de collegeverklaring. Dit assurance-rapport heeft betrekking op een subset van dit normenkader voor afnemers. Het betreft een dertiental normen. De Suwi-regelgeving steunt sterk op het principe van de horizontale verantwoording. Het gemeentebestuur heeft haar verantwoordelijkheid rond het gebruik SUWInet te nemen.

Praktijk is dat werkzaamheden in het domein werk- en inkomen belegd kunnen zijn bij diverse samenwerkingsverbanden. Deels werken deze onder mandaat, deels op basis van delegatie.

Ongeacht de organisatie van de samenwerkingsverbanden blijft het gemeentebestuur verantwoordelijk voor het gebruik SUWI. SZW verwacht van gemeenten dat zij ook in het geval samenwerking de bestuurlijke verantwoordelijkheid blijven nemen. De verantwoordingssystematiek gaat dan ook uit van het principe dat gemeenten verantwoording afleggen aan de toezichthouder. De daarvoor relevante informatie moeten zij bij eventuele samenwerkingsverbanden ophalen en verwerken. Binnen de ENSIA-tooling zijn daarvoor mogelijkheden gecreëerd.

In de praktijk blijken de afspraken tussen samenwerkingsverbanden en gemeenten zich vooral te richten op financiële performance en correcte afhandeling van werkprocessen. Het onderwerp informatieveiligheid is veelal niet belegd in de afspraken tussen gemeenten en samenwerkingsverbanden. Wel zullen in het kader van Wpb verwerkersovereenkomsten beschikbaar zijn.

Zorgpunten

Idealiter zouden gemeenten moeten kunnen steunen op de kwaliteit van informatiebeveiliging bij een samenwerkingsverband. In het ideale geval is dit vormgegeven doordat het samenwerkingsverband dit aantoont op basis van een daarop gericht assurance-rapport (TPM). In de praktijk zal dat echter niet het geval zijn. Op dit moment al wordt de projectorganisatie ENSIA door gemeenten benaderd met de vraag in hoeverre het uitvoeren van een op de Suwinormen gerichte audit bij het samenwerkingsverband zou moeten worden uitgevoerd en er dus ook bij het samenwerkingsverband een assurance-rapportage moet worden opgeleverd. De gemeentelijke auditor zou daar dan op moeten kunnen steunen.

In het ideale geval moeten alle betrokkenen daar wel naar streven en gemeenten en samenwerkingsverbanden in die richting doen opvoeden en de betreffende afspraken vast te leggen in overeenkomsten. Het is op dit moment te laat om dit steunende principe op te nemen in het nu voorliggende verantwoordingsstelsel. Vanuit de projectorganisatie ENSIA wordt een onderzoek gestart om deze situatie te verhelderen en vervolgens op te lossen. De op dit moment bestaande situatie is wat dat betreft van tijdelijke aard.

Dat ontslaat gemeenten en auditors overigens niet van de verplichting om wel een oordeel te hebben over de wijze waarop (al dan niet binnen de samenwerking) invulling wordt gegeven aan de voor SUWI relevante normen en de vertaling daarvan in de collegeverklaring. Immers dat is ook het leidende principe van ENSIA. Alle betrokkenen dringen er echter wel op aan om in dit stadium te zoeken naar een voor gemeenten en samenwerkingsverbanden pragmatische uitvoering.

Pragmatiek in de uitvoering

Het volgende is inmiddels ingeregeld in de verantwoordingssystematiek.

- Gemeenten (niet samenwerkingsverbanden) verantwoorden zich over gebruik SUWI op basis van een gedeelte van het normenkader afnemers
- De BIG en dat normenkader zijn gesynchroniseerd
- De ENSIA verantwoordingssystematiek (en de onderliggende tooling) is ingericht volgens dit principe
- Het vullen van deze tooling (en bijbehorende dossiers) is belegd bij de gemeentelijk coördinator. Deze coördinator heeft handvatten gekregen vanuit de tooling en het implementatieteam zodat deze verantwoording gevuld kan worden vanuit gemeentelijk perspectief.
- Door de auditor wordt vanuit gemeentelijk perspectief assurance gegeven op de gemeentelijke collegeverklaring. De ingevulde tooling en bijbehorende dossiers zijn daarvoor het uitgangspunt.
- Gemeenten wordt ten stelligste aangeraden om één auditor in te schakelen voor de in het samenwerkingsverband samenwerkende auditors. Onbekend is overigens of ze dat ook daadwerkelijk doen.

De audit in uitvoering

De meest pragmatische werkwijze lijkt dat de IT-auditor blijft werken vanuit gemeentelijk perspectief, dus:

- Zich een beeld vormt van de wijze waarop de gemeentelijk coördinator de totstandkoming van de collegeverklaring heeft vormgegeven en kan steunen op de gemeentelijke organisatie
- Zich een beeld vormt van de wijze waarop de informatie vanuit samenwerkingsverbanden in de gemeentelijke zelfevaluatie is verwerkt
- De aansluiting tussen collegeverklaring en onderliggende zelfevaluatie toetst
- Met de gemeentelijk coördinator en samenwerkingsverband afstemt welke gemeenten mogelijk gebruik maken van een andere auditor.
- Concreet: Eén auditor neemt de lead voor het toetsen van 13 normen bij het samenwerkingsverband in de vorm van een Richtlijn 3000-opdracht (TPM). Vooraf dienen de werkzaamheden met de collega-auditoren worden afgestemd. Afsluitend aan de werkzaamheden rapporteert de IT-auditor hierover aan zijn collega-auditoren.
- Vooraf kan het samenwerkingsverband alle relevante ENSIA- normen rapporteren / invullen in de ENSIA-tool. Dit staat los van de werkzaamheden van de IT-auditor. Wenselijk is dat de uitkomst van deze lijst overeenkomt met de werkzaamheden van de IT-auditor.

Bijlage 7 Begrippenkader

Aansluitbeleid	Onder aansluitbeleid wordt verstaan het beleid aangaande de bescherming van de eigen informatiehuishouding van de gemeente in relatie tot de eigen delen van Suwinet en de via Suwinet ter beschikbaar gestelde gegevens (bron: Specifiek Suwinet-normenkader Afnemers d.d. 1.01.2017)
Afnemer	De partij die de Suwigegevens gebruikt voor de uitvoering van haar wettelijke taken (de gemeente).
Applicatieleverancier	Een organisatie die een webapplicatie levert en die conform gemaakte afspraken verantwoordelijk is voor het onderhoud en de eventuele doorontwikkeling aan de software.
Bestaan	Het functioneren van een stelsel van informatiebeveiligings- en beheersingsmaatregelen conform beschrijving op of rond een peildatum.
Carve out methode	Bij de carve out methode wordt in een assurance rapport (zoals een DigiD assessment) een verwijzing opgenomen naar het assurance-rapport (de TPM) van een leverancier. De auditor van het assurance rapport en de auditor van de leverancier houden ieder zelfstandig hun vaktechnische verantwoordelijkheid. De eerste auditor dient wel vast te stellen dat de scope van beide rapportages in voldoende mate op elkaar aansluit.
Hosting leverancier	Een organisatie die conform gemaakte afspraken ICT-infrastructuur inclusief internettoegang aanbiedt waarop een webapplicatie kan worden uitgevoerd en kan worden aangeboden aan gebruikers.
Houder DigiD aansluiting	De organisatie die bij Logius staat geregistreerd als de verantwoordelijke voor een specifieke DigiD aansluiting. Iedere DigiD aansluiting wordt gekenmerkt door een uniek aansluitnummer. Per aansluitnummer is er een houder.
Inclusive methode	Bij de inclusive methode worden alle beheersmaatregelen in een assurance rapport overgenomen en er wordt dus niet verwezen naar de van derden verkregen assurance-rapporten (TPM's) waar eventueel gebruik van is gemaakt. De auditor van het assurance-rapport is vaktechnisch volledig verantwoordelijk en voert indien nodig een dossierreview uit voor een assurance-rapport waarvan de resultaten worden overgenomen.

Opzet	De beschrijving van een stelsel van informatiebeveiligings- en beheersingsmaatregelen.
Penetratietest	Dit is een specifieke vorm van een vulnerability-assessment. Het is een proces waarbij met behulp van technische hulpmiddelen specifieke componenten of specifieke delen van de ICT-infrastructuur op zwakheden gecontroleerd worden. (NCSC) In de context van het DigiD assessment wordt met een penetratietest een technisch beveiligingsonderzoek bedoeld dat vanaf het internet wordt uitgevoerd door een (ervaren) penetratietester en waarbij scantools worden ingezet en aanvullende handmatige onderzoeks-werkzaamheden worden uitgevoerd.
SAAS leverancier	Een organisatie die een webapplicatie als online dienst aanbiedt waarbij de klanten de software niet hoeven aan te schaffen. De aanbieder draagt zorg voor onderhoud en doorontwikkeling van (de software van) de applicatie, hosting en applicatiebeheer.
Third Party Mededeling (TPM)	Een TPM is een assurance-rapport dat betrekking heeft op een leverancier (serviceorganisatie) waarbij de doelgroep van het rapport een andere is dan de serviceorganisatie en de assurance wordt gegeven door een onafhankelijke auditor. Hierbij wordt opgemerkt dat de aanduiding Third Party Mededeling of TPM geen grondslag kent in de regelgeving van NOREA. In dit document is daarom telkens verwezen naar de term assurance-rapport onder opname van de term TPM aangezien deze term in de praktijk nog veel wordt gebruikt door alle bij ENSIA betrokken organisaties.
User control considerations (UCC)	In de UCC paragraaf in een assurance-rapport (TPM) worden beheersingsmaatregelen (controls) beschreven waarvan de betreffende leverancier aangeeft dat de gebruikersorganisatie (bijvoorbeeld een gemeente) deze moet hebben ingericht teneinde het stelsel van beveiligings- en beheersingsmaatregelen bij de leverancier optimaal te laten functioneren.
Vulnerability assessment	Dit is een proces waarbij met behulp van technische hulpmiddelen wordt nagegaan in hoeverre in de ICT-componenten kwetsbaarheden voorkomen waarvan ongeautoriseerden gebruik zouden kunnen maken (NCSC). In de context van het DigiD assessment wordt een (bij voorkeur geautomatiseerde) scan bedoeld die vanaf een intern netwerksegment zo dicht mogelijk bij de server wordt uitgevoerd op bekende kwetsbaarheden en ontbrekende patches.

Bijlage 8 Afkortingenlijst

BAG	:	Basisregistraties Adressen en Gebouwen
BIG	:	Baseline Informatiebeveiliging Nederlandse Gemeenten
BGP	:	Bruto Gemeentelijk Product = rekenfactor gebaseerd op Verklaringsmodel Lokale Economie
BGT	:	Basisregistratie Grootschalige Topografie, digitale kaart waarop gemeenten infrastructuur op éénduidige wijze moeten vastleggen
BRP	:	Basisregistratie Personen
BZK	:	(ministerie van) Binnenlandse Zaken en Koninkrijksrelaties
DigiD	:	Digitale Identiteit (voor overheidsdiensten en zorgverleners)
ENSIA	:	Eenduidige Normatiek Single Information Audit
GeVS	:	Gezamenlijke elektronische Voorziening Suwinet
ISAE-3000	:	International Standard on Audit Engagements 3000 (ook wel COS/Richtlijn 3000)
NCSC	:	Nationaal Cyber Security Centrum
PUN	:	Paspoort Uitvoeringsregeling Nederland
SOS	:	Security Officer Suwinet
Suwi(net)	:	Netwerk voor gegevensuitwisseling tussen overheidsorganisaties op basis van de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen
SZW	:	(ministerie van) Sociale Zaken en Werkgelegenheid
VNG	:	Vereniging van Nederlandse Gemeenten