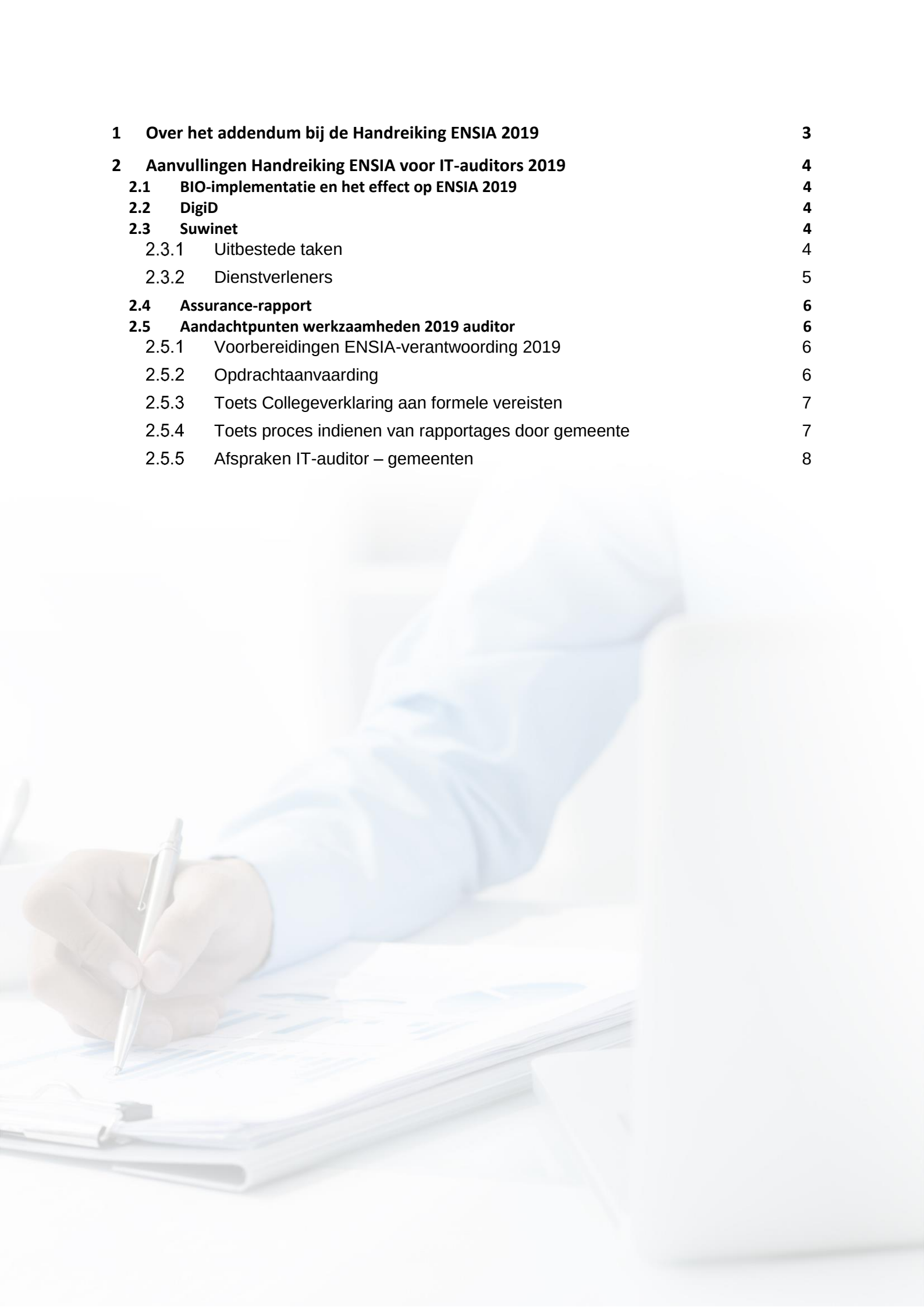
NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

ADDENDUM
Ten behoeve van werkzaamheden over 2019

HANDREIKING ENSIA voor IT-auditors (RE's)

Eénduidige Normatiek Single Information Audit voor gemeenten

Versie 1.0, 20 november 2019



1 Over het addendum bij de Handreiking ENSIA 2019

Beheer
Het addendum bij de handreiking ENSIA 2019 is uitgegeven door NOREA, de beroepsorganisatie van IT-auditors in Nederland. Het addendum bevat handreikingen voor de auditor specifiek gericht op ENSIA. Het betreft meer in het bijzonder de werkzaamheden van de auditor in het kader van het opstellen en controleren van de Collegeverklaring en bijlagen over het verantwoordingsjaar 2019. alsmede het daarbij af te geven assurance-rapport en bijlagen.

Het addendum maakt integraal deel uit van de Handreiking ENSIA 2019 en is bedoeld als guidance-document voor de IT-auditors die zich bezighouden met het project Eénduidige Normatiek Single Information Audit (ENSIA) voor gemeenten.

In het kader van het afstemmen van verwachtingen wordt de handreiking (inclusief het onderhavige addendum) ook ter beschikking gesteld aan de ENSIA-coördinatoren van gemeenten.

De handreiking is afgestemd op de Notitie verantwoordingsstelsel ENSIA (versie 11 juni 2019) en bijbehorende Handreikingen voor het verantwoordingsproces 2019 (zie https://www.vngrealisatie.nl/ensia), zoals vastgesteld in het overleg van de Regiegroep ENSIA
De handreiking inclusief het addendum mag worden gebruikt en/of gedistribueerd, mits met bronvermelding.

Voor vragen en opmerkingen over de Handreiking en het onderhavige addendum 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

Versiebeheer

Versie	Datum	Toelichting
Versie 0.1	21 oktober 2019	t.b.v. vaststellen Handreiking 2019 besloten actualia uit Handreiking te halen en separaat te laten vaststellen. E.e.a. tegen achtergrond actuele ontwikkelingen.
Versie 0.2	31 oktober 2019	Verrijkt met aandachtspunten uit updatesessie ENSIA d.d. 28-10-2019
Versie 0.3	7 november 2019	Na verwerking opmerkingen Werkgroep ENSIA / Vaktechnische Commissie
Versie 1.0	20 november 2019	Definitief na bespreking governance-organen ENSIA.

2 Aanvullingen Handreiking ENSIA voor IT-auditors 2019

2.1 BIO-implementatie en het effect op ENSIA 2019

ENSIA 2019 is een overgangsjaar naar de invoering van de BIO als baseline voor informatiebeveiliging door overheidsorganisaties. Door middel van pilots in 2019 wordt de BIO vertaald naar richtlijnen en de handreikingen ENSIA 2020 (waaronder de Handreiking ENSIA voor IT-auditors).

Vanwege de komst van de Baseline Informatiebeveiliging Overheid (BIO) als baseline over verantwoordingsjaar 2020, is door de Regiegroep ENSIA voor verantwoordingsjaar 2019 besloten tot beperkte aanpassingen in de verantwoordingsprocessen. Over het verantwoordingsjaar 2019 richten de Collegeverklaring (verantwoording) en de IT-audit zich op de DigiD-normen en een selectie van Suwinet normen wat betreft de opzet en het bestaan van voldoende maatregelen.

Op basis van het bovenstaande is een beperkt aantal wijzigingen doorgevoerd in de handreiking ENSIA. Deze zijn hoofdzakelijk van tekstuele aard. Deze geactualiseerde versie van de Handreiking is separaat beschikbaar gesteld aan de auditors en andere belanghebbenden.

2.2 DigiD

De in Bijlage 1 van de Handreiking ENSIA (versie 2.7 – update 2019) opgenomen "Guidance bij de te onderzoeken normen DigiD" geldt voor de IT-auditors als handvat voor de uitvoering van de auditwerkzaamheden. De NOREA werkgroep DigiD assessments beveelt IT-auditors daarnaast aan om bij de uitvoering van DigiD Assessments de maatregelen vanuit het *"Addendum Handreiking bij DigiD-assessments 2.0 (update 2019). Aanbevelingen technische beveiliging websites 6 september 2019, versie 1." te inventariseren. De uitkomsten daarvan kan de IT-auditor gebruiken* om de verantwoordelijke partij, daar waar relevant, te kunnen adviseren om deze maatregelen te treffen. Deze maatregelen zijn voor de DigiD Assessment 2019 nog niet verplicht, maar deze worden mogelijk wel onderdeel van het raamwerk voor 2020. Deze aanbevelingen zijn gebaseerd op de laatste inzichten omtrent de kwetsbaarheden en technische beveiliging van websites.

De handreiking DigiD-assessments en het addendum zijn terug te vinden op de website van het NOREA.

Ontwikkeling: Eind 2019, begin 2020 komt de werkgroep DigiD assessments met een volledig herziene Handreiking DigiD assessments 3.0. Deze zal met ingang het verantwoordingsjaar 2020 of later van toepassing zijn.

2.3 Suwinet

2.3.1 *Uitbestede taken*

Bij uitbesteding door de gemeente aan een externe partij (samenwerkingsverband / externe leverancier / combinatie van beide) heeft het de voorkeur dat de externe partij zorg draagt voor een verantwoording en een bijbehorend assurance-rapport afgegeven door een gekwalificeerde IT-auditor (conform Richtlijn 3000).

De verantwoording van de externe partij dient minimaal de verantwoording te bevatten over de relevante normen die van toepassing zijn op de door de gemeente bij deze partij neergelegde taken. Het assurance-rapport bevat de uitkomsten van een assurance-opdracht op basis van de in het kader van ENSIA gestelde normen.

Het heeft de voorkeur de nieuwe afspraken, vooruitlopend op de formele besluitvorming terzake, expliciet te baseren op de carve-out methodiek. In het assurance-rapport (voor de opdrachtgevende partij) dient de IT-auditor, waar van toepassing, een verwijzing op te nemen naar het assurance-rapport van de externe partij volgens de carve out methodiek.

Gemeenten dienen, voor het tijdig verkrijgen van het assurance-rapport / assurance-rapporten van de externe partij(-en) / samenwerkingspartners, hiertoe vooraf afspraken te maken met de externe partij. E.e.a. geldt ook voor de samenwerkingspartners van gemeenten indien zij voor hun werkzaamheden van externe partijen gebruik maken. Op de website van het NOREA is een *"TEMPLATE NOREA Assurance-rapport uitbestede Suwi-taken"* beschikbaar die de auditor van de externe partij / samenwerkingspartner als uitgangspunt kan gebruiken.

Gemeenten zijn ook in het geval van uitbesteding aan en / of samenwerking met andere organisaties integraal verantwoordelijk voor alle van toepassing zijnde normen voor alle Suwinet-aansluitingen en dienen hier verantwoording over af te leggen in de ENSIA tool.

Over het definitief toepassen van de carve-out methodiek dient door de Regieraad ENSIA nog een besluit genomen te worden. Daarbij zal ook een impact-analyse, over de implicaties van de invoering ervan voor gemeenten in het algemeen en ENSIA in het bijzonder, betrokken worden. De impact-analyse zal beschikbaar gesteld worden op de website van de VNG. IT-auditors kunnen deze hanteren in het kader van de advisering aan de verantwoordelijke partij.

Dit houdt in dat voor verantwoordingsjaar 2019 nog de **inclusive methode** wordt gehanteerd en de gemeente dus ook het assurance rapport van de externe partij niet separaat zal hoeven te uploaden in de ENSIA tool.

Gemeenten (waar nodig ondersteund door VNG-Realisatie) wordt geadviseerd nieuwe afspraken met externe partijen te baseren op de carve-out methodiek. Het hanteren ervan staat het nemen van de integrale verantwoordelijkheid (inclusief het afleggen van verantwoording over de uitgevoerde Suwinet-taken) niet in de weg.

Gelet op het feit dat 2019 een overgangsjaar is dient de auditor extra aandacht te besteden aan de tussen de gemeente en de samenwerkingspartners / dienstverleners gemaakte afspraken. Dit geldt in het bijzonder voor die situaties waarin reeds sprake is van de toepassing van de carve-out methodiek. Het is daarbij o.a. van belang vast te stellen dat:

- Er een overeenkomst is met de samenwerkingspartner / dienstverlener;
- De scope van de dienstverlening helder is;
- De samenwerkingspartner / dienstverlener (een verantwoording en) een assurance-rapport afgeeft over de dienstverlening;
- De daarin verantwoorde c.q. beoordeelde beheersmaatregelen kunnen worden gerelateerd aan Suwinet normen voor ENSIA;
- Inzichtelijk is welke beheersmaatregelen nog (aanvullend) bij de gemeente / opdrachtgever moeten worden beoordeeld.

Meer informatie omtrent uitbesteding door gemeenten is opgenomen in paragraaf 2.10 van de handreiking.

2.3.2 *Dienstverleners*

Organisaties die Suwi-taken uitvoeren maken in een aantal gevallen gebruik van dienstverleners die de beschikbare Suwi-informatie bewerken. Hierbij is sprake van verschillende rollen (bijvoorbeeld 'informatie-broker') en werkwijzen (bijvoorbeeld shared servicecentrum, dienstverleners die zelf delen van de werkzaamheden aan derden hebben uitbesteed), maar ook softwareleveranciers die in hun applicatie DKD Inlezen voor Suwi ondersteunen. Ingeval van het gebruik dient assurance over aanvullende norm items (GITC) te worden gegeven zoals in de hoofdtekst van de Handreiking beschreven.

De gemeente dient in het kader van het ENSIA-proces, bij de zelfevaluatie en het opstellen van de Collegeverklaring aandacht te besteden aan de uitbestede Suwi-taken en werkzaamheden.

De auditor dient hieraan in het kader van de assurance-werkzaamheden gericht op de Collegeverklaring vast te stellen dat deze informatie correct is weergegeven in de Collegeverklaring 2019 en de bijbehorende bijlagen.

Ontwikkeling: VNG-realisatie is in overleg met de dienstverleners om te komen tot verantwoordingen over de uitgevoerde werkzaamheden en een bijbehorende assurance-rapport (conform Richtlijn 3000 (bij voorkeur 3000A) of ISAE 3402 type 1 of 2) over de door deze dienstverleners uitgevoerde taken / werkzaamheden.

Hierbij zal sprake zijn van een groeipad waarbij het streven erop gericht is dat alle hiervoor bedoelde dienstverleners een verantwoording, inclusief bijbehorende assurance-rapportages, beschikbaar hebben die in het kader van ENSIA gebruikt kunnen worden.

2.4 Assurance-rapport

Voor de ENSIA-audit is door NOREA gekozen voor een structuur van het assurance-rapport welke aansluit bij de door de NBA (Nederlandse Beroepsorganisatie van Accountants) als afgeleide van NOREA Richtlijn 3000. Voor de goede orde zij vermeld dat voor het jaar 2019 geen aanpassingen zijn doorgevoerd in de gekozen bewoordingen.

Ontwikkeling: Onderzocht wordt op welke wijze de bewoordingen van het assurance-rapport in de toekomst beter kunnen aansluiten op de geuite wensen om de bestuurlijke hanteerbaarheid van de ENSIA-documenten te verbeteren zonder daarbij de eisen uit de controlestandaarden los te laten.

Eventuele aanpassingen in de bewoordingen van de Collegeverklaring en het assurance-rapport zullen eerst over het verantwoordingsjaar 2020 worden doorgevoerd.

2.5 Aandachtpunten werkzaamheden 2019 auditor

De ervaringen met ENSIA over de verantwoordingsjaren 2017 en 2018 zijn door alle partijen geëvalueerd. Op basis daarvan is een aantal expliciete / aanvullende aandachtspunten voor de auditor geformuleerd.

2.5.1 *Voorbereidingen ENSIA-verantwoording 2019*

In de Handreiking uitvoering ENSIA-verantwoording 2019 en bijbehorende documenten van de VNG wordt de gemeente geadviseerd rond het uitvoeren van de verschillende werkzaamheden, van zowel de gemeente als de IT-auditor, tijdig afstemming te zoeken met de direct betrokken partijen (samenwerkingspartners, dienstverleners en IT-auditor).

In dit kader verdient het eveneens aanbeveling dat de gemeente vaststelt over welke aansluitingen men beschikt die betrokken moeten worden in de ENSIA-verantwoording:

- Voor DigiD-aansluitingen is deze informatie te verkrijgen bij Logius;
- Voor Suwinet-aansluitingen is deze informatie te verkrijgen bij BKWI[1].

Vereist is dat de auditor vaststelt dat de gemeente de betreffende informatie heeft ingewonnen en dat de relevante aansluitingen betrokken zijn in het ENSIA-proces.

2.5.2 *Opdrachtaanvaarding*

In het kader van de opdrachtaanvaarding neemt de auditor de Richtlijn opdrachtaanvaarding in acht. Hierbij wordt o.a. nagegaan of de governance bij de gemeente voldoende waarborgen biedt voor het uitvoeren van de ENSIA-audit, waaronder:

- De opdracht wordt verstrekt door het verantwoordelijke lid van het college, de gemeentesecretaris of de verantwoordelijke directeur bedrijfsvoering;
- De ENSIA-coördinator:
  - een duidelijk mandaat heeft;
  - een directe escalatiemogelijkheid heeft naar de verantwoordelijke directeur bedrijfsvoering, gemeentesecretaris en het verantwoordelijke collegelid;
  - beschikt over voldoende ervaring met het uitvoeren van zelfevaluaties (meer in het bijzonder ENSIA);
  - bij voorkeur in dienst is van de gemeente.

[1] Het betreft hier een overzicht in opbouw. Informatie-uitwisseling met de gemeenten zal leiden tot een verdere aanvulling van de betreffende registratie bij BKWI.

Van belang is het daarbij op te merken dat de ENSIA coördinator via een door de gemeentesecretaris ondertekend formulier -waarin het bovenstaande weliswaar in andere bewoordingen is geregeld- dient te zijn aangemeld bij VNG-R. Het verdient derhalve aanbeveling dit formulier op te nemen in het auditdossier.

Indien hier niet in voldoende mate invulling aan is gegeven door de gemeente, dan is sprake van verhoogd risico en dient de auditor aanvullende (detail-) werkzaamheden te verrichten (met extra budget) om voldoende zekerheid te verkrijgen.

De opdracht moet uiteraard, conform de 'Richtlijn Opdrachtaanvaarding', schriftelijk bevestigd tussen gemeente en de voor de assurance-opdracht eindverantwoordelijke IT-auditor.

2.5.3 *Toets Collegeverklaring aan formele vereisten*

De auditor voert nauw overleg met de gemeente over het opstellen van de Collegeverklaring inclusief bijlagen en toetst het concept aan de gestelde eisen aan de Collegeverklaring en de bijbehorende bijlagen 1 en 2.

Zie hiervoor ook paragraaf 2.5 Pre-audit ENSIA van de Handreiking ENSIA voor IT-auditors voor een nadere toelichting.

2.5.4 *Toets proces indienen van rapportages door gemeente*

Het (tijdig, volledig en juist) indienen van de Collegeverklaring inclusief bijlagen en het assurance-rapport inclusief bijlagen is de verantwoordelijkheid van de gemeente.

De auditor gaat na in het kader van de assurance-werkzaamheden, gericht op de Collegeverklaring en bijlagen, of door de gemeente adequate maatregelen zijn getroffen rond het (adequaat) inrichten en afwikkelen van dit proces.

Het controleren of de gemeente het juiste Assurancerapport upload in de ENSIA tool valt buiten het kader van de assurance-werkzaamheden om te komen tot een oordeel over de Collegeverklaring en bijlagen. In overleg met partijen vertegenwoordigd in het Audit Committee ENSIA is afgesproken dat de auditor zelf vaststelt dat de juiste rapportages tijdig en volledig zijn / worden ingediend. Dit omdat dan de betreffende rapportages formeel aan de toezichthouders ter beschikking worden gesteld en daarbij aan bepaalde formele eisen moet worden voldaan. Een extra check door de auditor op dit proces voorkomt mogelijk later in het proces vragen. Hierover dienen nadere afspraken gemaakt te worden tussen de gemeente en de IT-auditor

Aandachtspunten hierbij zijn:

- Het opnemen van de juiste referentienummers;
- Het opnemen van de juiste kruisverwijzingen;
- Juist verantwoorden van de verdeling van werkzaamheden tussen gemeente en derde partijen (auditor en auditor derde partijen);
- Het opnemen van de van derde partijen ontvangen assurance-rapporten (alleen DigiD)
- Juistheid en volledigheid van de door de gemeente opgebouwde documentatie;
- Het waarmerken van stukken[2]

Hoewel de IT-auditor in dit kader nogmaals betrokken is bij de indiening van de rapportages; staat dit los van de afgegeven assurance-verklaring en heeft de auditor dan ook **geen** extra verplichtingen om vast te stellen of eventuele gebeurtenissen na rapportagedatum hebben plaatsgevonden die van invloed zouden kunnen zijn op de Collegeverklaring en bijbehorende bijlagen en / of (de strekking van) het door de IT-auditor afgegeven assurance-rapport.

De hier beschreven werkzaamheden van de IT-auditor zijn eenmalig van aard en uitsluitend van toepassing voor de werkzaamheden over het verantwoordingsjaar 2019.

[2] Waaronder het opnemen van het juiste referentienummer van het assurance-rapport van de auditor in de bijlage DigiD.

.

2.5.5 *Afspraken IT-auditor – gemeenten*

Indien en voor zover de bovengenoemde aandachtspunten niet zijn meegenomen in de afspraken die door de auditor met de gemeente zijn gemaakt rond het uitvoeren van de ENSIA-audit dienen hierover aanvullende afspraken gemaakt te worden.

Deze aanvullende afspraken dienen eveneens schriftelijk te worden vastgelegd in lijn met de schriftelijke opdrachtbevestiging van de gemeente aan de auditor.