ENSIA

Het audit perspectief

René IJpelaar
Achmed Bouazza
Werkgroep ENSIA

ENSIA | Eén slimme verantwoording voor informatieveiligheid

4 juli 2017

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Agenda

- Even voorstellen
- Uitgangspunten ENSIA
- Auditproces ENSIA voor de IT auditor
- Aandachtspunten bij het auditproces (Algemeen / DigiD specifiek / Kwaliteitsbeheersing)
- Wat doet NOREA
- Openstaande / nog op te lossen punten
- Vragen

Even voorstellen – Achmed Bouazza RE CISA

- 16+ jaar ervaring als IT auditor
- Sinds 6,5 jaar bij Mazars (Senior Manager)
- Expertise op het gebied van:
  - Assurance opdrachten (ISAE 3402, TPM's)
  - Web application security / DigiD assessments
  - IT audits ihkv de jaarrekeningcontrole
- Betrokken bij ENSIA Pilots sinds eind 2016
- Lid van NOREA werkgroep ENSIA en redactielid 'De IT–Auditor'

Even voorstellen – René IJpelaar RE CISA CEH

- 17 jaar werkzaam als IT auditor
- Sinds 5 jaar bij BKBO als oprichter
- Expertise op het gebied van:
  - DigiD assessments
  - Ethical Hacker
  - Suwinet audits
  - Baseline Informatiebeveiliging Gemeenten
  - ISO27001
  - Privacy Impact Assessments
- Betrokken bij ENSIA Pilots sinds eind 2016
- Lid van NOREA werkgroep ENSIA en DigiD

Uitgangspunten ENSIA

- Single Audit gedachte → 1 normenkader en 1 IT audit
- Normenkader gebaseerd op de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten)
- 7 objecten van onderzoek voorzien:
  - BIG
  - DigiD (Digitale Persoonsidentificatie) → in scope voor IT assurance 2017
  - SUWInet (Structuur Uitvoeringsorganisatie Werk en Inkomen) → in scope voor IT assurance 2017
  - BRP (Basisregistratie Personen)
  - PUN (Paspoortuitvoeringsregeling)
  - BAG (Basisregistratie Adressen en Gebouwen)
  - BGT (Basisregistratie Grootschalige Topografie)

Auditproces ENSIA voor IT auditor 1/2

- Gemeentelijke coördinator ENSIA stelt tijdens **zelfevaluatie** dossier samen voor BIG, BRP, PUN, BAG, BGT en voor DigiD en SUWInet (laatste 2 in scope voor assurance rapport 2017)

- 2 momenten van uploaden zelfevaluatie door gemeente (via ENSIA tool):
  - **1 oktober** voor BRP en PUN
  - **31 december** voor de rest / volle breedte BIG (incl. DigiD en SUWInet)

- Gemeente kiest o.a. IT auditor en autoriseert deze → Aparte template voor opdrachtverlening in ontwikkeling

- IT auditor neemt voor DigiD en SUWInet kennis van ingevulde zelfevaluatie via ENSIA tool plus de geüploade TPM('s)

- ENSIA coördinator levert dossier met evidence aan IT auditor **buiten de tooling om**

- IT auditor komt langs in Q1 2018 voor formele toetsing van DigiD en SUWInet normen
  - Diepgang: **Opzet en Bestaan**
  - In latere jaren kan scope en diepgang ook werking gaan betreffen (streven NOREA)

Auditproces ENSIA voor IT auditor 2/2

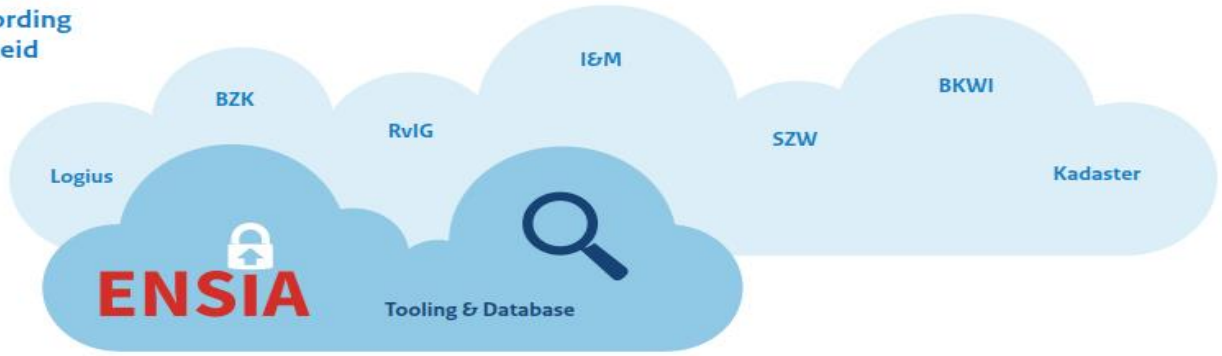
- ENSIA zelfevaluatie heeft een “brede” scope, echter de gemeente stelt collegeverklaring op voor verantwoording aan gemeenteraad over de voor 2017 geselecteerde normen voor SUWInet en DigiD
  - IT auditor beoordeelt alleen DigiD en SUWInet voor 2017
  - In collegeverklaring worden naast SUWInet alle DigiD aansluitingen waar de gemeente houder van is tezamen verantwoord

- IT auditor geeft daarbij een verklaring bestaande uit:
  - Assuranceverklaring bij collegeverklaring onder ISAE 3000 A
  - Bijlage A met uitgevoerde werkzaamheden, bevindingen en aanbevelingen (gaat niet mee in tooling)

- Wat wordt geüpload in ENSIA voor stakeholders :
  - Collegeverklaring (1)
  - Assuranceverklaring IT auditor (1)
  - Bijlagen B & C per DigiD aansluiting
  - TPM(‘s) per DigiD aansluiting

- Deadline rapportage IT auditor is nog steeds **1 mei 2018**

ENSIA | Eén slimme verantwoording voor informatieveiligheid



Proces ENSIA verantwoordingsjaar 2017

Het College van B&W is verantwoordelijk voor de organisatie en uitvoering van het ENSIA verantwoordingsproces.

01-07-2017
Vragenlijst zelfevaluatie beschikbaar.

Inhoud vragenlijst en scope IT-audit jaarlijks vastgesteld in strategisch beraad.

Peildatum 01-10-2017
Inleveren vragenlijst **BRP** en **PUN**.

Peildatum 31-12-2017
Inleveren antwoorden voor zelfevaluatie over de volle breedte **BIG** (met inbegrip van **DigiD**, **SUWInet**, **BAG** en **BGT**)

Q1 2018
Opstellen van de Collegeverklaring informatie-beveiliging.

01-05-2018
Uploaden Assurance rapport en Collegeverklaring informatiebeveiliging.

Uploaden rapportage **BAG** en **BGT**.

Uiterlijk 15-07-2018
Het College van B&W legt verantwoording over informatie-veiligheid af aan de gemeenteraad.

Gemeentelijke coördinator ENSIA

De gemeente organiseert het ENSIA verantwoordingsproces, bijvoorbeeld via een gemeentelijk coördinator. De coördinator zorgt voor het intern uitzetten en tijdig aanleveren van de zelfevaluatie vragenlijst. Ook zorgt de coördinator ervoor dat er onder andere een Collegeverklaring informatiebeveiliging wordt opgesteld, er één IT-audit wordt uitgevoerd en een Assurance rapport wordt opgeleverd.

IT-auditor

De gemeentelijke coördinator ENSIA zoekt tijdig contact met IT-auditor.

Op basis van de resultaten uit de zelfevaluatie vragenlijst en de Collegeverklaring informatiebeveiliging wordt een IT-audit uitgevoerd en een Assurance rapport opgeleverd. De scope van de IT-audit in 2017 omvat DigiD en SUWInet.

Aandachtspunten Auditproces ENSIA – Algemeen

- Gemeenten dienen tijdig een IT auditor te selecteren → Er komt een template opdrachtverlening

- Gemeentelijke coördinatoren dienen getraind te worden om audit evidence op te leveren

- IT auditor dient zich vooraf te verdiepen in nieuwe normeringen DigiD en SUWInet → **Guidance DigiD beschikbaar, guidance SUWInet wordt aan gewerkt en wordt in september verwacht**

- Het is aan te bevelen om een nulmeting / proefaudit voorafgaand aan de formele audit uit te voeren, in samenwerking met de gemeente → **rol voor IT auditor!**

Aandachtspunten Auditproces ENSIA – DigiD specifiek

- Nieuwe DigiD normen 2.0 → Guidance reeds beschikbaar
- Gemeentelijke samenwerkingsverbanden die DigiD houder zijn leggen direct aan Logius verantwoording af, zoals nu al het geval is
  - Gemeenten kunnen afspraken maken met samenwerkingsverbanden over wijze van verantwoording
- Aansluitvoorwaarden DigiD van Logius blijven van kracht:
  - Binnen 2 maanden DigiD rapport aan Logius bij nieuwe aansluiting
- Logius ontvangt met assurancerapport ook verklaring over SUWInet → willen ze liever niet, wordt besproken tussen Logius en BZK
- Tijdens zelfevaluatie (okt– dec) dienen gemeenten reeds antwoord te geven over TPM vragen DigiD terwijl deze nieuwe TPM er mogelijk nog niet is → Nog niet helder/duidelijk hoe hiermee omgegaan wordt

Aandachtspunten Auditproces ENSIA – Kwaliteitsbeheersing

- Zorg voor goede dossiervorming
- In Bijlage A (DigiD) aangeven wat de uitgevoerde werkzaamheden zijn geweest en welke detailbevindingen en aanbevelingen er zijn
- Nagaan op welke wijze collegiale toetsing / review kan plaatsvinden

Wat doet NOREA?

- NOREA werkgroep ENSIA ingesteld sinds mei 2017 (voorzitter: Peter Verstege)
- Subwerkgroepen voor Oordeelsvorming en Guidance ingesteld (geleid door resp. Peter Verstege en Maarten Mennen)
- Voorlichtingssessies en opleidingen voor IT auditors inzake ENSIA regelen
- Contact onderhouden met BZK, VNG en Logius omtrent vaktechnische en organisatorische vraagstukken

Openstaand / Nog op te lossen (1/2)

- **COMPLEX VRAAGSTUK:** Hoe om te gaan met **oordeelsvorming** inzake DigiD en SUWInet voor 2017, bijv.:
  - oordeel per norm vs overkoepelend oordeel
  - één oordeel over twee objecten; SUWInet en DigiD
  - meerdere DigiD aansluitingen vs overkoepelend oordeel
  - presentatie voor de lezer / bewoordingen / geen onterechte assurance aan ontlenen
  - uniforme uitvoering door auditors
  - publieksvriendelijke verwoording versus vaktechnische vereisten
  - etc.

- Guidance vanuit Werkgroep NOREA wordt in oktober verwacht

- Verzoek aan eenieder om vragen uit de praktijk zsm te delen met de werkgroep voor tijdige afstemming met BZK / VNG

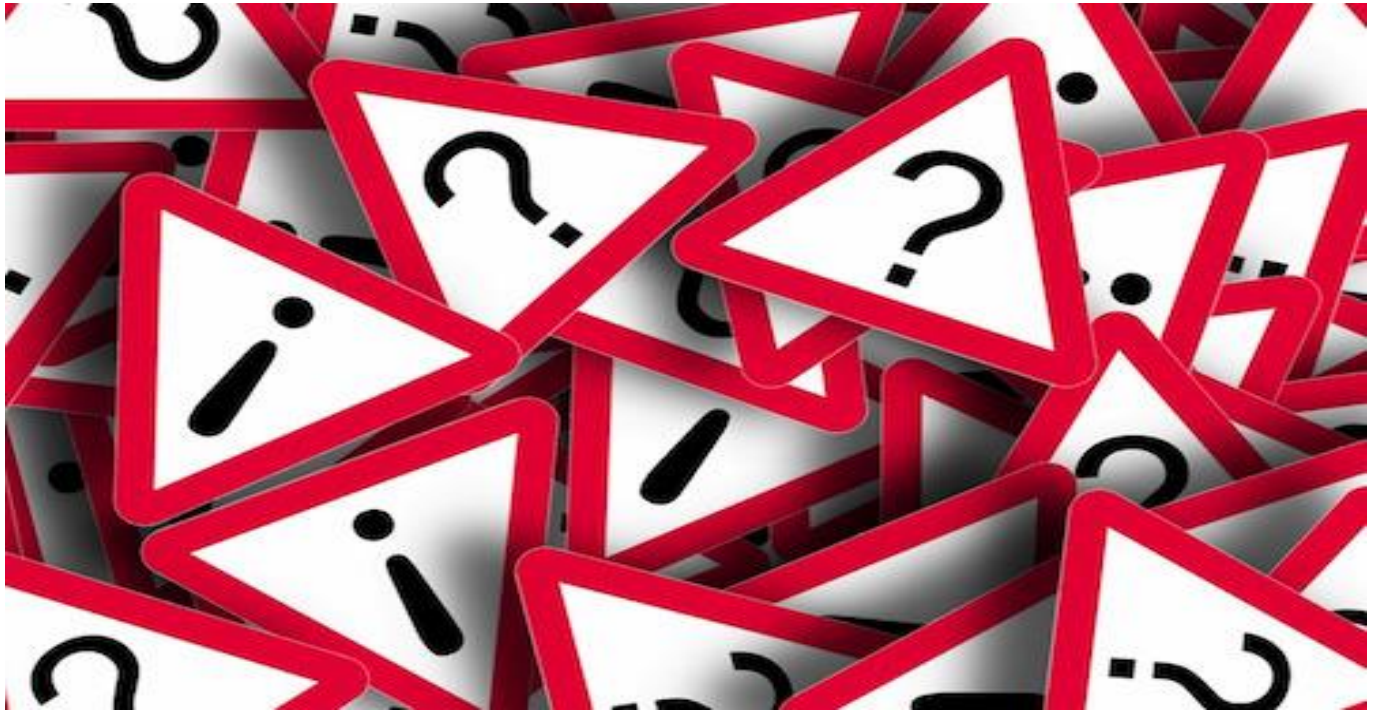
Openstaand / Nog op te lossen (2/2)

- Hoe om te gaan met TPM's tijdens zelfevaluatie?
- In jaarverslag gemeente wordt een paragraaf Informatiebeveiliging opgenomen die verwijst naar de zelfevaluatie ENSIA → wat zal de rol van de accountant hierbij zijn?
- Diverse vragen vanuit de deelnemers van de Werkgroep en de praktijk

Tot slot

- Subwerkgroepen Oordelen (okt) en Guidance SUWInet (sept) komen vroeg in najaar met nadere informatie
- Volgende voorlichtingssessie uiterlijk in november met nadere toelichting
- NOREA Werkgroep ENSIA vraagt IT auditors om eventuele vragen / ervaringen / issues te delen met werkgroep

Vragen?



Bedankt

Voor meer informatie kun je contact opnemen met:

René IJpelaar
rene@bkbo.nl
06 – 28978955

Achmed Bouazza
achmed.bouazza@mazars.nl
06 – 43994867

NOREA werkgroep ENSIA

Peter Verstege (voorzitter)
PVerstege@deloitte.nl

Maarten Mennen (plv. voorzitter)
mjgmennen@rsm-nl.nl

4 juli 2017

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS