ENSIA voor Informatieveiligheid

Informatie voor Auditors

04072017

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

ENSIA: Wat vooraf ging…

Resolutie ‘Informatieveiligheid een randvoorwaarde voor professionele dienstverlening’

- Implementatie Baseline informatieveiligheid gemeenten (BIG)
- Visitatiecommissie
- Verklaring in het jaarverslag voor de gemeenteraad
- Stroomlijnen van (departementale) audit – en verantwoordingslast

In deze presentatie

- Principes en uitwerking ENSIA
- De Rotterdamse praktijk
- Hoe helpen we gemeenten
- Consequenties voor audit

ENSIA de basis

- Gemeenten verantwoorden zich aan de **eigen toezichthouder**.
- Gemeenten voeren **zelfevaluatie informatieveiligheid** uit.
- Via één **tool**
- Rapporteren over informatieveiligheid op basis van zelfevaluatie in **jaarverslag gemeenten.**

- Gemeenten stellen **Collegeverklaring** op, het '**Assurance-rapport**' sluit hierop aan
- Er vindt **één ENSIA-audit** plaats (over DigiD en Suwi).
- Landelijk toezichthouders maken gebruik van de gemeentelijke verantwoording

Wat heeft de gemeente eraan?

- Door ENSIA heeft het gemeentebestuur overzicht over hun informatieveiligheid
- Zo kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad
- Verantwoordingsprocedure wordt efficiënter en overzichtelijker.
- Gegevens over informatieveiligheid en niet-informatieveiligheid worden op één moment uitgevraagd
- Geharmoniseerd normenkader voor informatieveiligheid
- Verantwoordingsinformatie wordt nog maar één keer verzameld
- Er is nog maar één ENSIA audit (Digid en Suwi)

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.

Horizontale verantwoording

Het is aan **individuele** gemeenten om, gebruikmakend van deze ondersteuning, het horizontale verantwoordingsproces in te richten, zodat in **zoveel mogelijk** gemeenten:

- In het jaarverslag een paragraaf informatieveiligheid is opgenomen
- In het verslag van de raadsvergaderingen het onderwerp ‘informatieveiligheid’ is opgenomen
- Binnen gemeenten waar nodig verbeteracties zijn geformuleerd en belegd (opgenomen in inhoud Collegeverklaring)
- De aanzet is gegeven voor borging van het ENSIA-verantwoordingsproces bij gemeenten

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.

Verticale verantwoording

dat in **alle** gemeenten:

- een Collegeverklaring wordt opgesteld (DigiD Suwi)
- door de auditor ‘assurance’ is gegeven en deze Assurance rapportage aansluit bij de in ENSIA-verband afgesproken scope in de stuurgroep
- de voor verticale toezichthouders relevante informatie op het vlak van informatie-veiligheid is geleverd conform de met hen gemaakte afspraken.

Verantwoordingsstelsel

- Verantwoordingsparagraaf Informatiebeveiliging
- Collegeverklaring (scope DigiD en Suwi)
- Assurancerapport auditor
  - Gebaseerd op Collegeverklaring
  - Over beide onderwerpen
  - In toekomst meer richten op horinzontale aspecten

In deze presentatie

- Principes en uitwerking ENSIA
- De Rotterdamse praktijk
- Hoe helpen we gemeenten
- Consequenties voor audit

Rotterdam in (IB) beeld!

- **Bas de Wit RE / Vanaf 2010 bij R'dam (Concern Auditing)**

- **Wat trof ik aan.. Verschillende individuele verantwoordingen**
  - BRP / PUN / BAG / BGT
  - Suwi (2x: suwipartijen / niet-suwipartijen: niet uit te leggen)
  - DigiD
  - Maar ook.. ITGC, et cetera (risk base, opdrachten)

- **Hoe het ging**
  - Elk een eigen audit- / verantwoordingsregime en normenkader…
  - Stimuleert ook niet tot eenduidige IB processen.. Vanuit deze sectorale normeringen veelvoud aan specifieke IB policies en beleidsplannen.. Dat kan beter!
  - Van 'Diensten' naar '1Concern'

- **Hoe het gaat**
  - Dat gaat ook beter.. Audits brengen wel wat teweeg (DigiD / ISMS), IB beleid en plannen in samenhang..
  - Naast ENSIA ook ander 'externe' stimuli!
  - Aandacht vanuit de rekenkamer en raad
  - Privacy (Implementatie AVG / Datalekken)
  -

Implementatie Ensia R'dam

- **Regie en coördinatie ENSIA (Tvb's)**
  - Governance IB ("aansluiten P&C / verantwoordingscyclus")
  - Wie doet wat (30), deadlines, coördinatie, uitvoering en rapportage
- **Proces zelfevaluatie BIG (ciso / diso / lijn)**
  - ZE BRP / PUN; DigiD; Suwi; BAG / BGT; Consolidatie en rapportage
- **Proces bestuurlijke verantwoording (staf / lijn / college)**
  - Collegeverklaring ENSIA, *Paragraaf IB tbv verantwoording Raad*, opstellen begroting
- **Audit ENSIA (DigiD, Suwi)**
  - Opdrachtgever (GS, ..), gedelegeerd opdrachtgever (Lijn, IB)
  - Opdrachtnemer CA
  - Uitvoeren: Q1 2018 (mikken op eerste onderzoek naar de 'opzet' van de normen in Q4 2017)
  - Samenhang en samenwerking
- **Aandachtspunten**
  - Sloepentest huidige verantwoordingen ("Geen verassingen")
  - Horizontale verantwoording ('BIG breed' / ITGC / Privacy / AVG)
- **(Privacy) governance / IB-control → P&C cyclus (PDCA/ISMS)**

IB in control

Zijn we veilig.. of

Hebben we de belangrijkste IB eisen en risico’s in grip en kunnen we dat aantonen

In deze presentatie

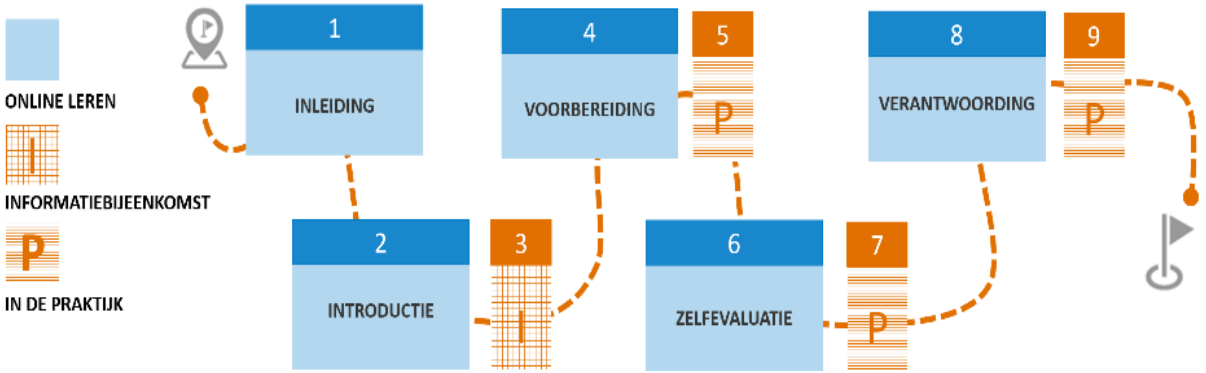
- Principes en uitwerking ENSIA
- De Rotterdamse praktijk
- Hoe helpen we gemeenten
- Consequenties voor audit

Ondersteuning

- Leeromgeving
  - Stappenplan
  - Formats
  - Handreikingen
- Procesbegeleiding
- Helpdesk
- ENSIA op agenda van bestuurders

Coördineren van het ENSIA-verantwoordingsproces

Stappenplan



Stappenplan

- Fase I: Voorbereiding (1 april tot 1 juli 2017)
  - Benoemen coördinator en aanmelden
  - Aanmelden voor leeromgeving en regiobijeenkomst
  - Opstellen plan van aanpak
  - Kick-off bijeenkomst
  - Autorisaties inregelen voor ENSIA-tooling
- Fase II: Zelfevaluatie (1 juli tot 31 december 2017)
  - Verlenen auditopdracht
  - Tijdig betrekken auditor bij evaluatieproces
  - Beoordelen en uploaden TPM's DigiD
- Fase III: Verantwoording (1 januari tot 15 juli 2018)
  - Paragraaf informatieveiligheid
  - Opstellen collegeverklaring
  - Ondersteunen auditor
  - Uploaden assurancerapport

Procesbegeleiders

Wijnand Heijnen

Renee Musch

Sanneke van der Linden

Chris Deben

Jeanne-Marie Langen

In deze presentatie

- Achtergrond/Aanleiding
- Principes en uitwerking ENSIA
- De Rotterdamse praktijk
- Hoe helpen we gemeenten
- Consequenties voor audit

Audit

- Horizontaal verantwoordingsproces is de basis
- Verticale verantwoordingen steunen
- Assuranceverplichting alleen voor
  - DigiD
  - Suwi

DigiD

- Nieuw Normenkader
- Richtlijn Norea integraal opgenomen in tooling ENSIA; geeft handvatten aan coördinator.
- Beoordeling normen én tpm in eerste instantie door coördinator ENSIA van gemeente
- Tijdige aanlevering TPM’s
- Ondersteuningsaanbod ENSIA coördinatoren in leeromgeving
- Criterium aansluithouder is leidend.
- Tooling realiseert bijlagen B en C uit Norea richtlijn én geeft input Collegeverklaring
- Deadline nog steeds 1 mei

SUWI

- Basis is SUWI normenkader voor afnemers
- Met SZW afspraken over de normen die worden voorzien van Assurance (in lijn met de zeven essentiele normen inspectie)
- Beoordeling normen eerste instantie door coördinator ENSIA van gemeente
- Guidance SUWI opgenomen in tooling
- Tooling levert met BKWI afgestemde gegevens voor invulling norm C08 (transparantie)
- Systematiek afgestemd met Ministerie SZW en NOREA
- Deadline 1 mei

Bedankt

Voor meer informatie kun je contact opnemen met:

Peter van Dijk
Peter.vandijk@vng.nl
0622493064

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS