FACTSHEET

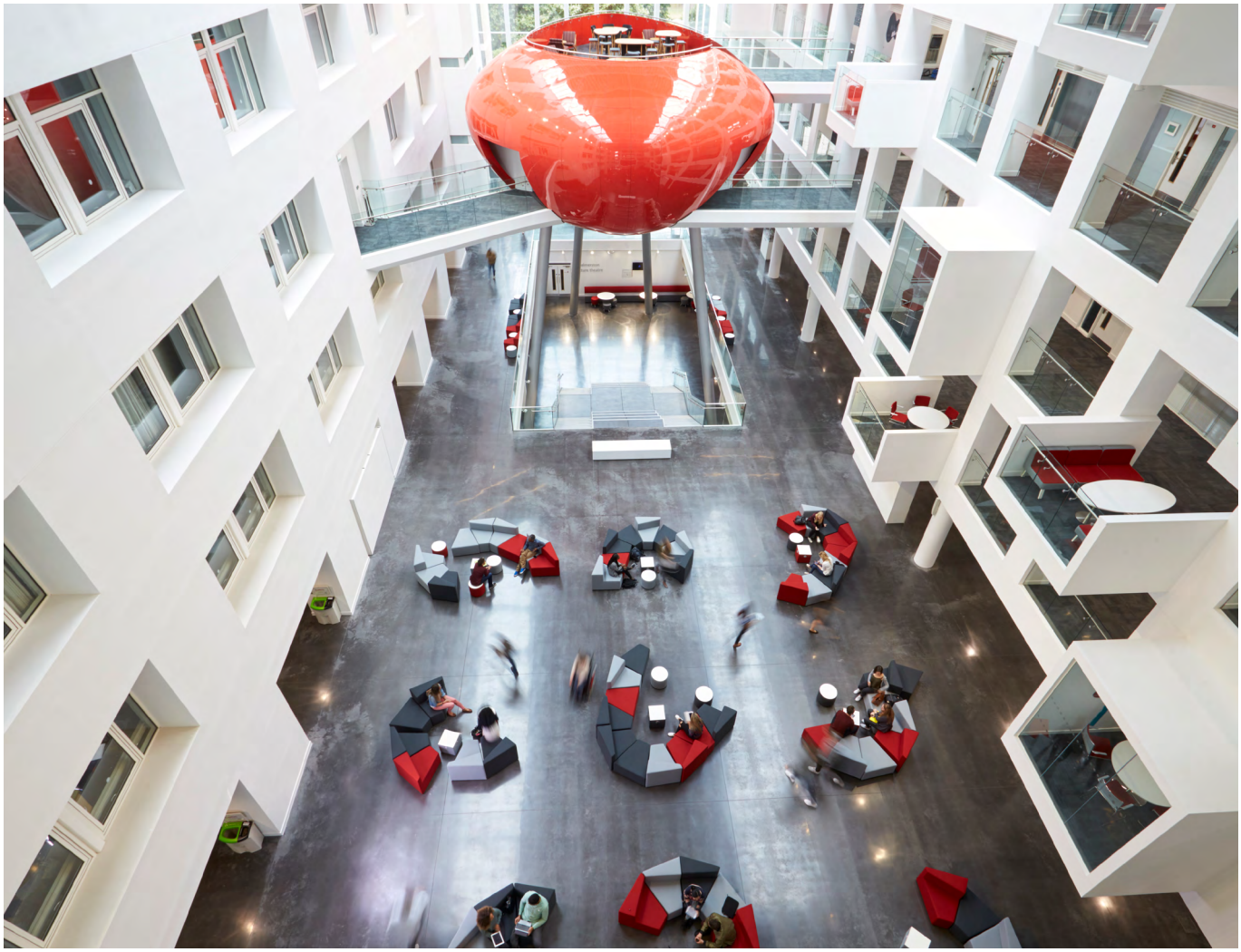
ENSIA-regelgeving biedt gemeenten kansen

Nieuwe ENSIA-regelgeving biedt gemeenten de kans het proces rondom de verplichte aantoonbaarheid van informatieveiligheid te optimaliseren. De sterk toegenomen en nog steeds toenemende digitalisering van gemeenten vraagt veel aandacht voor de kwaliteit van informatieveiligheid. Gemeenten beheren onder andere veel persoonsgegevens en dat worden er door decentralisatie van overheidstaken alleen maar meer. Elk jaar moeten gemeenten zich dan ook verantwoorden over de kwaliteit van informatieveiligheid en/of de hierbij gebruikte informatiesystemen/-platformen.

Tot nu toe bestonden hiervoor diverse aparte audits; een tijdrovende aangelegenheid voor gemeenten. Het project ENSIA (Eenduidige Normatiek Single Information Audit) heeft als hoofddoel de verantwoording voor gemeenten te vereenvoudigen door deze zo effectief en efficiënt mogelijk in te richten, gebaseerd op de Baseline Informatieveiligheid Nederlandse Gemeenten (BIG).

Opbouw verantwoordings-systematiek

De BIG vormt de kern van de horizontale verantwoording aan de gemeenteraad. In 2017 dient elke gemeente een zelfevaluatie op te stellen en uit te voeren door middel van het invullen van een vragenlijst. Op basis van de uitkomsten van de zelfevaluatie



wordt een collegeverklaring opgesteld waarop een audit plaats zal vinden. De scope van de audit voor 2017 betreft Suwinet en DigiD. Zo wordt 'horizontaal' de collegeverklaring (waarin de gemeente de algehele status van informatieveiligheid verantwoordt) in het jaarverslag verwerkt, om deze vervolgens als integraal rapport aan te bieden aan het ministerie van Binnenlandse Zaken. 'Verticaal' wordt de specifieke status per auditonderdeel (voor 2017 Suwinet en DigiD) verantwoord richting de betreffende toezichthouder (bijv. Logius voor DigiD). De rapportagedeadline hiervoor is 1 mei 2018.

De verantwoording zal via de ENSIA-tooling plaatsvinden waarin gemeenten op digitale wijze rapportages en informatie beschikbaar stellen over de zelfevaluatie, de collegeverklaring en het assurancerapport aan de desbetreffende ministeries.

Concreet

Met ENSIA krijgt het college meer inzicht in de stand van zaken van de informatieveiligheid, kan het beter sturen op informatieveiligheid en kan het daarover verantwoording afleggen aan de gemeenteraad. Hiervoor zijn wel enkele uitgangspunten van groot belang:

- De implementatie van ENSIA is per 1 juli 2017 van start gegaan;
- Er is een zelfevaluatievragenlijst beschikbaar welke een basis vormt voor het opstellen van de collegeverklaring waarbij het college van B&W vaststelt of men aan de normen voldoet inzake informatieveiligheid;
- De ENSIA-coördinator van de gemeente levert een dossier met bewijsstukken aan bij de IT-auditor;
- De IT-auditor neemt voor DigiD en Suwinet kennis van de ingevulde zelfevaluatie via de ENSIA-tool en de aangeleverde bewijsstukken;
- De IT-auditor beoordeelt alleen DigiD en Suwinet voor 2017 en geeft daarbij een verklaring bestaande uit: assuranceverklaring bij de collegeverklaring onder de ISAE3000-richtlijn;
- Voor 15 juli 2018 legt het college van B&W verantwoording af over informatieveiligheid aan de gemeenteraad;
- Voor kalenderjaar 2018 is de verwachting dat meerdere audits (bijv. BRP, PUN en BAG) onderdeel zullen worden van de ENSIA-audit.

Onze diensten

Deze aangepaste verantwoordingsplicht van de gemeente vergt veel kennis en deskundigheid op het gebied van de eisen waaraan u als gemeente moet voldoen bij een ENSIA-audit. Om een beeld te krijgen van de huidige status van informatieveiligheid en/of de huidige kwaliteit van het verantwoordingsproces binnen de organisatie, alsook de stappen die nog genomen moeten worden om beide onderdelen op het juiste (vereiste) niveau te brengen, bieden wij de volgende diensten aan:

ENSIA Compliance Scan

Aan de hand van het normenkader dat is uitgegeven in opdracht van de overheid voeren wij een ENSIA Compliance Scan (hierna ECS) uit. Met een ECS stellen wij vast op welke punten u nog maatregelen moet treffen om aantoonbaar aan het normenkader te voldoen dat door de overheid verplicht is gesteld. Met deze uitkomst kunt u een actieplan opstellen om tijdig uw organisatie 'veiliger' in te richten, zodat u in het eerste kwartaal van 2018 hierop een controle kunt laten uitvoeren (ENSIA Assessment) door een register IT-/EDP-auditor (RE).

ENSIA Assessment

Met het ENSIA Assessment wordt de daadwerkelijke audit uitgevoerd aan de hand van het ENSIA-normenkader door de register IT-/EDP-auditor (RE). De hieruit voortkomende assuranceopdracht voeren wij uit over uw collegeverklaring aan de hand van de richtlijn ISAE3000. De assurancerapportage wordt samen met uw collegeverklaring digitaal verstrekt aan het ministerie van Binnenlandse Zaken via de ENSIA-tool. Daarnaast dient u de collegeverklaring integraal te betrekken in uw jaarverslag per juli 2018.

Hoe onze kennis u verder helpt

- Een gestandaardiseerde aanpak van de ENSIA-audit;
- Ruime ervaring op auditgebied specifiek bij gemeenten en andere lokale overheden;
- Grip op het gebied van informatieveiligheid en continuïteit van de bedrijfsvoering;
- Inzicht in concrete risico's die u loopt met informatieveiligheid;
- Voorbereid zijn op de implementatie van de ENSIA-audit;
- Antwoorden op complexe vraagstukken rond de impact van de ENSIA-audit op de verantwoording van informatieveiligheid naar derden;
- Concrete advisering over te treffen maatregelen ten behoeve van de ENSIA-audit;
- Verminderde kans op toezicht van de overheid;
- Voorkomen van reputatieschade als gevolg van non-compliance op het ENSIA-normenkader.

Meer weten?

De verantwoordingsvraagstukken zijn complex, hebben organisatiespecifieke impact en vragen op korte termijn al uw aandacht. Wij gaan daarom graag persoonlijk met u in gesprek over de wijze van ondersteuning die het best past bij uw huidige situatie. Wilt u hier een vrijblijvend gesprek over of meer informatie over dit onderwerp, neem dan contact op met één van onze specialisten via telefoonnummer 088 - 236 48 22.

Michiel Hopstaken
Manager IT Audit
T 06 – 235 22 075
E michiel.hopstaken@bdo.nl

Jarno Smit
Jr. Manager IT Audit
T 06 – 114 47 357
E jarno.smit@bdo.nl

10/2017 – PS1721