Haarlem

Informatienota

Onderwerp Informatievoorziening en -veiligheid in de P&C-cyclus	
Nummer	2017/534701
Portefeuillehouder	Spijk, J.K.N. van
Programma/beleidsveld	6.2 Gemeentelijk bestuur
Afdeling	CS/CC
Auteur	Raaphorst, H.
Telefoonnummer	023-5113614
Email	hraaphorst@haarlem.nl
Kernboodschap	In de auditcommissie van 19 september hebben de leden aangegeven nader geïnformeerd te willen worden over het inbedden van informatiebeheer en –veiligheid in de P&C-cyclus. Dit is een ontwikkelproces dat zich gezien de externe ontwikkelingen (de VNG is hier al sinds 2013 mee bezig), de organisatieverandering in 2018 (het adaptievermogen), het interne leerproces en het leerproces van verantwoorden over informatieveiligheid over meerdere jaren zal gaan uitstrekken. Deze informatienota schetst de contouren van de ontwikkelingen.
Behandelvoorstel voor commissie	Het college stuurt de informatienota ter kennisname naar de commissie Bestuur. De gemeente wil haar zelf controlerend vermogen versterken en self compliant zijn op zowel financieel gebied als ook op informatievoorzieningsgebied (IV/IT). Informatievoorziening zal daarom een grotere plaats krijgen in de Planning & Control-cyclus. Dit dwingt de organisatie om transparant te sturen en te verantwoorden, te verbeteren en deze verbeteringen te borgen. In de vergadering van de auditcommissie van 19 september 2017 is het inbedden van informatiebeheer en –veiligheid in de P&C-cyclus aan de orde geweest en op hoofdlijnen besproken. De commissie heeft aangegeven nader geïnformeerd te willen worden over de ontwikkelingen en deze informatie met de raad te willen delen. Met deze informatienota wil het college in die behoefte voorzien.
Relevante eerdere besluiten	N.v.t.
Besluit College d.d. 28 november 2017	1. Het college stelt de informatienota aan de commissie vast. de secretaris, de burgemeester,

Inleiding
De gemeente wil haar zelf controlerend vermogen versterken en self compliant zijn op zowel financieel gebied als ook op informatievoorzieningsgebied (IV/IT). Informatievoorziening zal daarom een grotere plaats krijgen in de Planning & Control-cyclus. Dit dwingt de organisatie om transparant te sturen en te verantwoorden, te verbeteren en deze verbeteringen te borgen. In de vergadering van de auditcommissie van 19 september 2017 is het inbedden van informatiebeheer en –veiligheid in de P&C-cyclus aan de orde geweest en op hoofdlijnen besproken. De commissie heeft aangegeven nader geïnformeerd te willen worden over de ontwikkelingen en deze informatie met de raad te willen delen. Met deze informatienota wil het college in die behoefte voorzien.

Kernboodschap
In de auditcommissie van 19 september hebben de leden aangegeven nader geïnformeerd te willen worden over het inbedden van informatiebeheer en –veiligheid in de P&C-cyclus. Dit is een ontwikkelproces dat zich gezien de externe ontwikkelingen (de VNG is hier al sinds 2013 mee bezig), de organisatieverandering in 2018 (het adaptievermogen), het interne leerproces en het leerproces van verantwoorden over informatieveiligheid over meerdere jaren zal gaan uitstrekken. Deze informatienota schetst de contouren van de ontwikkelingen.

ENSIA
Directe aanleiding voor het inbedden van informatiebeheer in de P&C-cyclus is het project ENSIA, wat staat voor Eenduidige Normatiek Single Information Audit. Vóór ENSIA als aanpak waren vanuit verschillende toezichthouders separate (verticale) verantwoordingsprocedures ingericht voor 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). Tussen deze verschillende verantwoordingsprocedures bestond noch een inhoudelijke, noch een chronologische samenhang. Elke toezichthouder was gewoon vanuit een eigen perspectief, met eigen prioriteit, in een eigen ritme, audits, inspecties en controles uit te voeren. Dit betekende een enorme versnippering, en daarmee ook een grote administratieve last, voor de gemeente, maar ook voor de toezichthouders zelf.

Door samenwerking van :
- Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties;

- Het Ministerie van Infrastructuur en Milieu;

- Het Ministerie van Sociale Zaken en Werkgelegenheid, en;

- De Vereniging van Nederlandse Gemeenten,

en met een uitvoerende rol voor het Kwaliteits Instituut Nederlandse Gemeenten (KING) zijn de verschillende verantwoordingsprocedures gebundeld in ENSIA. De eerste stappen om tot ENSIA te komen zijn reeds in 2013 gezet. Door ENSIA kunnen gemeenten vanaf 2017 in één keer slim, verticaal én horizontaal, verantwoording afleggen over het gebruik van de zes genoemde registratiesystemen.

Het oogmerk van ENSIA is, naast de verticale verantwoording, het regelen van horizontale verantwoording. Het college verantwoordt zich hierbij volgens dezelfde ENSIA methodiek aan de gemeenteraad. Het college geeft over de gehele reikwijdte van de ingevulde ENSIA vragenlijst een verklaring af in het jaarverslag. De juistheid en volledigheid van de collegeverklaring wordt getoetst door een IT-auditor[1], die, voor aanvullende zekerheid, een zogenaamde 'assurance verklaring' afgeeft. Het gemeentebestuur krijgt door ENSIA meer zicht op de informatieveiligheid binnen de gemeente en kan daarmee beter (bij-) sturen.

ENSIA wordt in 2017 voor de eerste maal ingezet en dat jaar wordt voor alle betrokken partijen geoormerkt als een 'leerjaar' waarbij ervaringen kunnen worden opgedaan. Naast het opdoen van de eerste ervaringen, is ENSIA op andere punten nog niet helemaal uitgekristalliseerd en wordt komende jaren nog doorontwikkeld. Ontwikkelingsrichtingen die nu al ter sprake worden gebracht:

- verbreding, waarbij naast de zes genoemde registratiesystemen mogelijk andere systemen in scope komen;

- verdieping, waarbij naast opzet en bestaan (huidige vorm) ook werking van (beheersings-) maatregelen in scope komt;

- verandering van de grondslag voor ENSIA, de Baseline Informatiebeveiliging Gemeenten (BIG), naar de Baseline Informatiebeveiliging Overheid (BIO). Waarbij één baseline gaat gelden voor de gehele overheid[2].

Meer informatie over ENSIA en ontwikkelingen daaromtrent is te vinden op www.ensia.nl en www.KINGgemeenten.nl.

2017

In het pré-ENSIA tijdperk was de externe verantwoording het beste te kenschetsen als een aantal onsamenhangende interne processen van verschillende afdelingen, veelal op projectmatige manier aangelopen. Met ENSIA en het benoemen van een ENSIA-coördinator is in 2017 het proces van (externe én interne) verantwoording samengebundeld in één collectieve inspanning, echter nog steeds met een projectmatig karakter. De projectmatige insteek voor 2017 is mede ingegeven door het nieuwe karakter van ENSIA waar (behalve binnen een aantal pilot-gemeenten) nog geen ervaring mee is opgedaan. Daarbij komt dat de (verplicht te gebruiken) ENSIA tooling nieuw is en nog een aantal 'kinderziekten' vertoont. In de tweede plaats ontbreekt op dit moment eenvoudigweg structurele inbedding in de thans bestaande P&C-cyclus. Over 2017 wordt ENSIA daarom nog buiten de P&C cyclus om aangelopen.

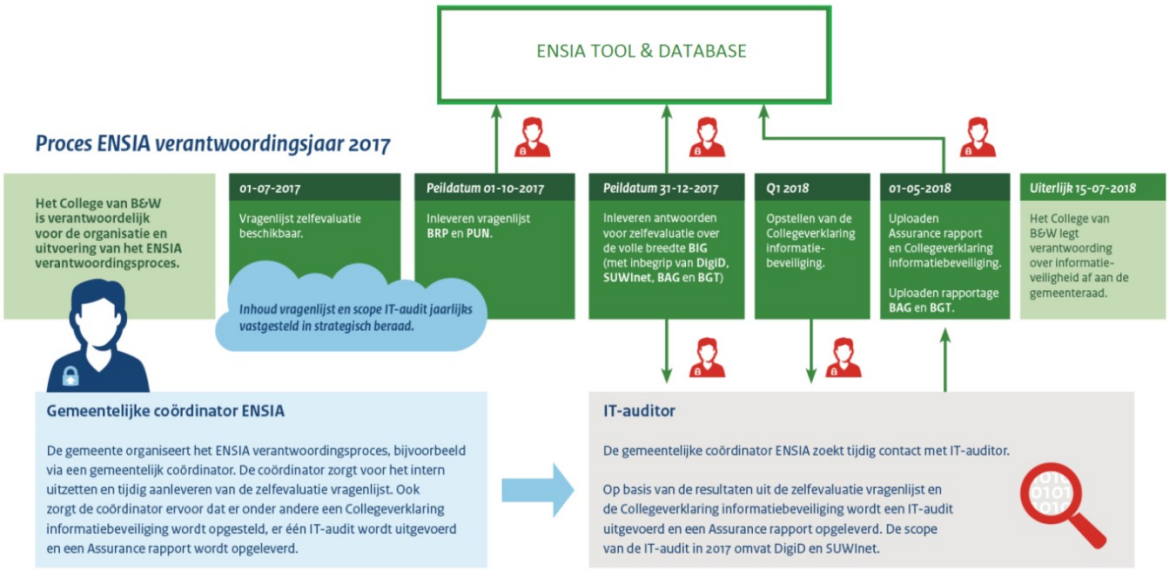
Producten die door ENSIA ontstaan zijn:

- Een voor 31 december 2017 volledig ingevulde ENSIA tool. Hierin wordt, onder aansturing door de ENSIA-coördinator, verantwoording afgelegd over de informatiebeveiliging met betrekking tot de zes hierboven genoemde domeinen. De inhoud van het tool dient voor het eind van het jaar te zijn 'geüpload' naar de ENSIA organisatie, die de inhoud aan de verschillende externe toezichthouders beschikbaar stelt;

[1] Een bij NOREA ingeschreven IT-Auditor (RE) die onder de beroeps- en gedragsregels van het Register valt.
[2] Thans hebben verschillende overheden nog hun eigen baseline voor informatiebeveiliging.

- Een collegeverklaring informatieveiligheid over de gehele reikwijdte in het jaarverslag[3];
- Een assuranceverklaring, type 3000A (attest) over de collegeverklaring met als scope DigiD en Suwinet.

Figuur 1: Proces ENSIA 2017



2018 - 2020

Informatiebeheer en –veiligheid is een aspect dat structureel aandacht dient te krijgen[4] en een onderdeel zou moeten vormen van de reguliere bedrijfsvoering. ENSIA stuurt hier ook op aan. De samenhang tussen interne (financiële) beheersing en informatiebeheer wordt sterker[5] naarmate de digitalisering voortschrijdt.

De interne bedrijfsvoering van de gemeente wordt steeds afhankelijker van een betrouwbare IV/IT. Dit stelt dan ook nadrukkelijk (hoge) eisen aan de beschikbaarheid, integriteit en vertrouwelijkheid van (geautomatiseerde) systemen. Naast burgers en bedrijven moeten ook de medewerkers van de gemeente kunnen vertrouwen op de betrouwbaarheid van de geautomatiseerde systemen die hen in hun werk ondersteunen. Informatiebeveiliging vormt daarmee meer en meer een integraal onderdeel van de bedrijfsvoering en dient dan ook breder te worden gezien als louter de zes domeinen die thans door de ENSIA bestreken worden. Naast het oogmerk van ENSIA, maakt ook de verbreding van informatiebeheer en –veiligheid naar bedrijfsvoering in algemene zin het noodzakelijk het verantwoordingsproces met betrekking tot informatiebeheer en –veiligheid aan te laten sluiten bij de gemeentelijke P&C-cyclus.

[3] Mogelijk wordt dit voor 2017 nog een collegeverklaring los van het jaarverslag. Begin november 2017 was opname in het jaarverslag een intentie, maar dit was nog niet definitief vastgesteld. Bedoeling voor 2018 e.v. is dat de collegeverklaring wel in het jaarverslag wordt opgenomen.

[4] Het Kwaliteits Instituut Nederlandse Gemeenten (KING), adviseerde in 2013 het aspect informatievoorziening een gewicht toe te kennen dat vergelijkbaar is met de verdeling van de beschikbare middelen: http://zorgendestad.digitalestedenagenda.nl/wp-content/uploads/sites/3/2014/01/eindadvies-visd-totaal-29-07-2013.pdf

[5] O.a.: Coalitieprogramma Haarlem 2014-2018 (digitalisering / informatieveiligheid); Visie op 100% digitaal werken; (anticiperen op) de Digitale agenda 2020

Door deze aansluiting ontstaat tevens een belangrijke randvoorwaarde voor structurele verbetering, borging (lerende organisatie) en (interne) informatievoorziening over deze onderwerpen aan de Raad(-scommissies).

P&C-cyclus
De gemeente Haarlem heeft, naast de ontwikkelingen rondom ENSIA, haar eigen ambities met betrekking tot digitalisering en de (beveiligings-)eisen die hier aan gesteld worden, geformuleerd. Het aantoonbaar en in continuïteit voldoen aan gestelde beveiligingsnormen en -eisen[6] is, naast horizontale en verticale verantwoording, een belangrijke reden om informatiebeveiliging op te nemen in de reguliere P&C-cyclus.
Zoals gezegd zal hier de periode 2018 - 2020 nader invulling aan worden gegeven. Eind 2017 is hiervoor een overleg ingericht met als hoofdonderwerp 'compliancy'. De aspecten informatiebeheer en –veiligheid vertonen in de praktijk grote overlap en samenhang, te samen met de aspecten privacy (AVG), integriteit en (mede door de hoge automatiseringsgraad) financieel beheer. Het is dan ook het meest efficiënt en effectief om deze aspecten in samenhang te beschouwen. In het compliancy overleg zal, na een initiële inventarisatie van relevante wet- en regelgeving en gehanteerde *best practices* (Haarlems beleid), via een meerjarige en cyclische[7] aanpak uitgewerkt worden hoe de bestaande P&C-cyclus verrijkt gaat worden met de hierboven genoemde aspecten.
Uitgangspunten voor die uitwerking:

- *Self-compliant* op alle organisatieniveaus: betrokkenen leggen (in de lijn) voor hun verantwoordelijkheidsgebied primair zelf actief verantwoording af;
- De primaire processen zo veel mogelijk 'ontzorgen': generiek wat kan, alleen specifiek wat moet;
- Geen blauwdruk, maar ontwikkelen in dialoog;
- Niet lineair, maar cyclisch ontwikkelen;
- (eind-)gebruikers staan van meet-af-aan centraal: aansluiting op sturings- en verantwoordingsbehoeften.

Audit
Aanvullend aan het uitgangspunt *self-compliant* is audit. ENSIA maakt hier bijvoorbeeld ook gebruik van. Een (IT) auditor verschaft aanvullende zekerheid (assurance) over hetgeen door het college verklaard wordt (2017: DigiD en Suwinet).
Audits worden binnen de gemeente echter breder ingezet dan voor ENSIA. Sinds jaar en dag voeren de interne financial auditors (accountants) al onderzoek uit naar het financieel beheer. In september 2017 heeft de gemeente ook een IT Auditor aangesteld, die de assurance verklaring in het kader van ENSIA gaat verzorgen. Audits zullen echter breder worden ingezet, waarbij onderzoek uitgevoerd wordt naar zowel de gehanteerde sturings- en verantwoordingswijze (governance) als naar de (IV/IT[8]) objecten. Die objecten kunnen zijn: projecten, processen en infrastructuur.

[6] Concreet: eisen aan beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid.
[7] Een cyclische aanpak, om tweede en derde orde leerprocessen mogelijk te maken, hetgeen uitmond in een 'lerende organisatie'.
[8] IV, informatievoorziening. IT, Informatietechnologie.

1+1=3
Het samenspel van een P&C-cyclus die (mede) gericht is op het actief sturen en monitoren op aspecten van informatiebeheer en –veiligheid en (IT-)Audit stelt het college in staat om:

- (pro-)actief te sturen;

- Transparant en betrouwbaar te verantwoorden;

- Als organisatie te leren en te ontwikkelen.