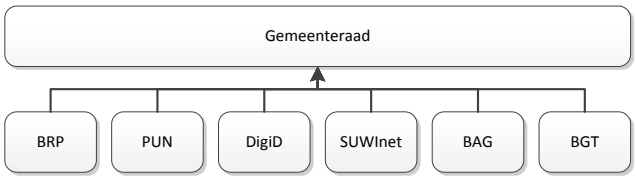
Verantwoordingsinformatie informatiebeveiliging en privacy

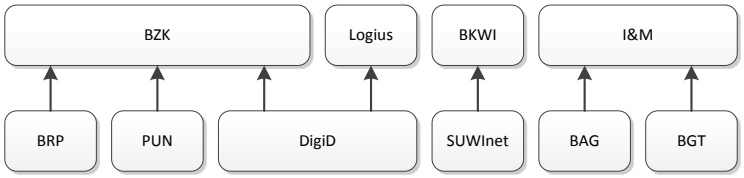
Inhoudsopgave

1 Inleiding

In 2017 is voor het eerst verantwoording afgelegd middels ENSIA (Eenduidige Normatiek Single Information Audit). ENSIA wordt gebruikt ten behoeve van horizontale verantwoording richting gemeenteraad en verticale verantwoording richting toezichthouders; er wordt over de gehele breedte verantwoording afgelegd richting de gemeenteraad en per onderwerp wordt verantwoording afgelegd richting toezichthouders.



Figuur 1: horizontale verantwoording



Figuur 2: verticale verantwoording

In de tweede helft van 2017 zijn vragenlijsten ingevuld om de stand van zaken voor de verschillende onderwerpen te bepalen:

- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- Basisregistratie Personen (BRP)
- Paspoortuitvoeringsregeling (PUN)
- Digitale persoonsidentificatie (DigiD)
- Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Adressen en Gebouwen (BAG)

1.1 Resultaten

Voor BRP en PUN is voor 1 oktober 2017 de zelfevaluatie uitgevoerd. Hierover is verantwoording afgelegd richting het Ministerie van BZK. Resultaten en actiepunten zijn gerapporteerd richting College van B&W (T17.40852).

DigiD en Suwinet zijn onderdeel van de Collegeverklaring informatiebeveiliging (I18.15655) en Assurance rapport (I18.15658) naar aanleiding van de IT-audit uitgevoerd door Mazars.

BAG en BGT komen aan de orde in Verantwoordingsrapportage BAG (Basisregistratie Adressen en Gebouwen) en BGT (Basisregistratie Grootschalige Topografie) ENSIA 2017 (BW1800173) en Raadsinformatiebrief (U18.04796)

Collegeverklaring, incl. bijlagen, assurancerapport en verantwoordingrapportage BAG en BGT zijn in de ENSIA-tool geupload, zodat deze beschikbaar komen voor de verticale toezichthouders.

Dit document licht de stand van zaken toe voor wat betreft informatiebeveiliging en privacy. Op verzoek van de raad wordt dit ditmaal in een separaat document opgenomen. Volgend jaar wordt dit onderdeel van het jaarverslag.

2 Verantwoordingsinformatie informatiebeveiliging en privacy

2.1 IB-beleid, doelstellingen en ambities

Doel van informatiebeveiliging volgens het informatiebeveiligingsbeleid is het behoud van beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid. Dit draagt bij aan de volgende doelstellingen:

- Het zorgvuldig en bewust omgaan met informatie
- Betrouwbare dienstverlening
- Beheersen van risico's
- Voldoen aan wet- en regelgeving

Gemeente Lansingerland heeft de ambitie om aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) te voldoen en verantwoording af te leggen middels Eenduidige Normatiek Single Information Audit (ENSIA).

Hierbij geeft de rekenkamer in haar onderzoeksrapport aan dat het voldoen aan de BIG geen doelstelling dient te zijn; maar dat de BIG in combinatie met risicoanalyses instrumenten zijn om bovenstaande doelstellingen te realiseren.

2.2 Samenvattend beeld en resultaten afgelopen periode

In 2017 zijn een Privacy-officer en een Chief Information Security Officer (CISO) aangesteld om de onderwerpen Privacy en Informatiebeveiliging de aandacht te geven die het verdient. Op het gebied van Informatiebeveiliging heeft in eerste instantie de focus gelegen op het opstellen en vaststellen van de informatiebeveiligingsprocedures in het kader van BIG-maatregelen, de uitvoering van de ENSIA (Eenduidige Normatiek Single Information Audit) en het Rekenkameronderzoek Informatiebeveiliging. Daarnaast is de start gemaakt met de bewustwording binnen de organisatie die we in 2018 volop doorzetten.

Ten aanzien van Privacy is tevens de start gemaakt met de bewustwording. Daarnaast is in kaart gebracht wat de nieuwe AVG inhoudt en wat de consequenties zijn. Als eerste stap is het Privacybeleid is opgesteld (vastgesteld in 2018). Gelijktijdig zijn we concreet aan de slag gegaan met de verwerkersovereenkomsten. Voor alle inkoopovereenkomsten in het sociaal domein zijn verwerkersovereenkomsten opgesteld.

Het onderzoeksrapport van de rekenkamer is gebruikt als input voor het maken van het uitvoeringsplan informatiebeveiliging.

Wat hebben we hiervoor gedaan?

- Naar aanleiding van een uitgevoerde risicoanalyse zijn 57 BIG-maatregelen geselecteerd. Hiervoor zijn procedures opgesteld en vastgesteld; waaronder de incidentenprocedure, de procedure datalekken en de procedure in- en uitdiensttreding. Daarnaast zijn we gestart met implementatie van bijv. wijzigingsbeheer.
- We hebben verantwoording afgelegd via ENSIA.
- We hebben ons de AVG eigen gemaakt en vertaald naar de consequenties voor onze organisatie.
- We hebben het Privacybeleid opgesteld (vastgesteld 1 feb 2018).

- We hebben de verwerkersovereenkomsten voor de inkoopovereenkomsten in het sociaal domein opgesteld.
- We hebben diverse bewustwordingsacties uitgevoerd: waaronder informatiebijeenkomsten en het gebruik van @work (intranet) met ‘prikkelende’ vragen.

2.3 Disclaimer

Het is goed om te beseffen dat 100% veiligheid niet bestaat. Er is altijd sprake van nieuwe ontwikkelingen waardoor nieuwe kwetsbaarheden kunnen ontstaan. Daarnaast hebben we te maken met de menselijke factor; mensen zullen altijd in staat zijn om maatregelen bewust of onbewust te omzeilen.

Het is onmogelijk om het risico helemaal tot nul terug te brengen. Op basis van geïdentificeerde risico’s treffen we maatregelen. Hierbij maken we continue de afweging of het beoogde doel de inzet van middelen rechtvaardigt.

2.4 Belangrijkste beheersmaatregelen IB

Zowel uit het Rekenkamer onderzoek als ENSIA blijkt dat er een aantal verbeterpunten is. Vanuit ENSIA zijn de belangrijkste verbeterpunten:

- Wijzigingsbeheer
- Afspraken met leveranciers / samenwerkingsverbanden
- Bewustwording
- Logische toegangsbeveiliging
- Fysieke toegangsbeveiliging
- Technische maatregelen
- Bedrijfscontinuïteit

Conclusies en aanbevelingen uit het Rekenkamer onderzoek komen in hoofdlijnen overeen met de hierboven genoemde verbeterpunten.

2.5 Realisatie doelstellingen IB-beleid (effectiviteit beheersmaatregelen en risico’s)

De eerder genoemde 57 geselecteerde BIG-beheersmaatregelen zijn in 2017 nog niet volledig geïmplementeerd. Dit wordt vervolgd in 2018.

De effectiviteit van beheersmaatregelen wordt intern nog niet gemeten; de focus ligt op het implementeren en borgen van de basis. Vervolgens zal de effectiviteit gemeten worden middels controles op de maatregelen.

In het onderzoek van de rekenkamer is de effectiviteit van maatregelen door een externe partij getoetst. De rekenkamer heeft op basis van de bevindingen een aantal aanbevelingen gedaan.

2.6 Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en Suwinet

Collegeverklaring ENSIA (I18.15655) inzake informatiebeveiliging DigiD en Suwinet zijn 24 april door het college van B&W vastgesteld. De IT-auditor heeft in het assurancerapport (I18.15658) beoordeeld dat de collegeverklaring juist is.

2.7 Incidenten

Voor het melden en afhandelen van informatiebeveiligingsincidenten en datalekken hebben we procedures.

Sinds het vierde kwartaal van 2017 worden informatiebeveiligingsincidenten en (potentiële) datalekken vastgelegd in ons meldingensysteem. Hierdoor wordt afhandeling, vastlegging en rapportage vereenvoudigd.

In 2017 zijn 55 informatiebeveiligingsincidenten gemeld. Een groot deel (38 stuks) vallen in de volgende categorieën:

- Meldingen over kwetsbaarheden van de Informatiebeveiligingsdienst voor Nederlandse Gemeenten (IBD) (17 stuks)
- Bevindingen uit het Rekenkamer onderzoek (14 stuks)
- Onterechte meldingen (7 stuks). Dit ging om testmeldingen en onterecht als informatiebeveiligingsincident ingedeelde meldingen

Bij de overige meldingen (17 stuks) ging het bijvoorbeeld om spam- en/of phishing mails die niet geblokkeerd werden, mails die onterecht geblokkeerd werden, technische kwetsbaarheden, onjuiste toegangsrechten op een netwerkschijf, etc.

Er zijn in 2017 zeven datalekken opgetreden. Hiervan zijn er drie gemeld bij Autoriteit Persoonsgegevens en de betrokkene(n). Al deze datalekken zijn veroorzaakt door menselijk handelen of het ontbreken hiervan.

2.8 Meerjarenperspectief

In 2018 gaan we verder met de implementatie van de eerder geselecteerde BIG-maatregelen. Deze zijn op basis van de uitkomsten van de uitgevoerde risicoanalyse geselecteerd.

Een deel van deze maatregelen zijn ook als verbeterpunten uit het rekenkamer onderzoek en ENSIA gekomen. Het is dus wenselijk om op deze ingeslagen weg verder te gaan.

Daarnaast volgen we de aanbevelingen uit het rekenkamer onderzoek op. Zoals eerder opgemerkt komen de verbeterpunten op hoofdlijnen overeen.

Naast de periodieke gemeentebrede risicoanalyse gaan we zogenaamde risicoanalyses uitvoeren op procesniveau. Doel is om te identificeren in welke situaties aanvullende beheersmaatregelen noodzakelijk zijn.

In februari 2018 is de conceptplanning uit Bijlage A gepresenteerd aan de raad. Op basis van bovenstaande maatregelen, aanbevelingen en eventueel aanvullende maatregelen die volgen uit risicoanalyses wordt de concept planning aangepast en wordt er een plan van aanpak opgesteld voor de rest van 2018 en 2019.

Bijlage A. Concept planning 2018

	2017				2018				2019
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
Implementatie BIG									
Opstellen procedures, etc.		x	x	x					
Implementatie procedures, borging & aantoonbaarheid					x	x	x		
Updaten en vaststellen beleid							x	x	
Bepalen implementatieplan (2018-2019)							x	x	
Uitvoeren implementatieplan								x	x
Aandachtspunten rekenkamer onderzoek									
Onderzoek			x	x					
Risk based aanpak									
Diepgaande risicoanalyse sociaal domein						x			
Scope en planning overige domeinen						x			
Uitvoeren						x	x	x	x
Bevindingen externe en interne pentest en inlooptest									
Zaken als "incidenten" oplossen				x	x				
Complexe wijzigingen (impact bepalen, etc.)					x	x	x	x	x
Voorkomen slordig omgaan met vertrouwelijke info (volgt o.a. uit risico analyses)						x	x	x	x
Bewustwording									
Campagne (incl. bevindingen social engineering test)					x	x	x	x	
Introductie nieuwe medewerkers						x	x	x	
E-learning training medewerkers						x	x	x	
Bespreken in team- /afdelingsoverleggen					x	x	x	x	
Hertest (social engineering, interne + externe pentest)							x		
ENSIA									
Zelfevaluatie BRP, PUN			x						
Zelfevaluatie BIG (incl. DigiD, Suwinet, BAG, BGT)				x					
Collegeverklaring & IT-audit					x	x			
Uploaden assurance report en collegeverklaring						x			
Verantwoording richting raad (mei)						x			

Figuur 3: concept planning