Informatieveiligheid

Onderzoeksopzet

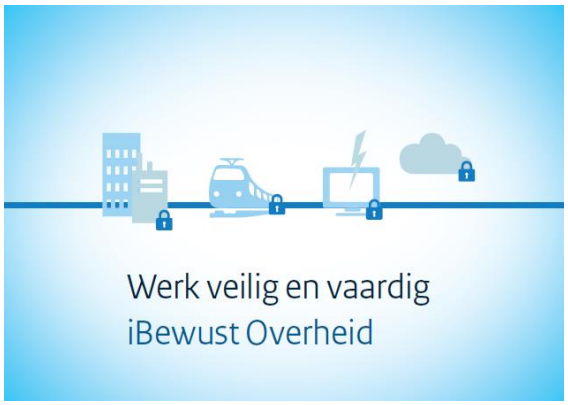
Amsterdam, september 2015

Inhoudsopgave

1. Aanleiding

De overheid en digitale informatieveiligheid

De dienstverlening van de overheid vindt in toenemende mate digitaal plaats. Ook voor provincies geldt dat zij voor de uitvoering van hun primaire taken steeds meer afhankelijk zijn van informatiesystemen en informatiestromen. Digitale veiligheid neemt dan ook een steeds belangrijker positie in.[1] Overheden hebben hierin een maatschappelijke verantwoordelijkheid: burgers, bedrijven en overheidspartners moeten erop kunnen rekenen dat de informatievoorziening betrouwbaar is en dat er zorgvuldig wordt omgegaan met gegevens. Een betrouwbare informatievoorziening is van essentieel belang voor het functioneren van de processen van de overheid.[2] Daarnaast speelt wet- en regelgeving een rol: de Wet Bescherming Persoonsgegevens en de Archiefwet, bijvoorbeeld, stellen eisen aan de verwerking en opslag van informatie. Nu is het zo dat datalekken van persoonsgegevens moeten worden gemeld bij het College bescherming persoonsgegevens. In aanvulling daarop treedt vanaf 1 januari 2016 de Meldplicht datalekken in werking, die geldt voor alle organisaties die persoonsgegevens verwerken. Deze meldplicht betekent dat bij een data-lek, waarbij kans is op verlies of onrechtmatige verwerking van persoonsgegevens, de betrokkene hierover geïnformeerd moet worden.[3] Daarnaast kunnen inbreuken op digitale veiligheid leiden tot grote financiële en imagoschade.[4] Uit onderzoek blijkt echter dat de helft van alle digitale inbraakpogingen vaak pas na maanden wordt ontdekt.[5] Daarnaast toonden het DigiNotar-incident en Lektober (2011) en het Dorifel-virus (2012) aan dat de digitale veiligheid van overheden een aantal kwetsbaarheden bevatte.[6]



Figuur 1 Bewustwordingscampagne iBewustzijn Overheid, een ondersteuningsprogramma van het ministerie van BZK en de koepelorganisaties om bewuste omgang met informatie door ambtenaren te stimuleren (Bron: www.iBewustzijnOverheid.nl)

Mede naar aanleiding van bovenstaande ontwikkelingen zijn er verschillende initiatieven genomen om de informatieveiligheid van overheden te verbeteren. Zo is in 2013 de Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID) opgericht, waarin het Rijk, het Interprovinciaal Overleg (IPO), de Vereniging Nederlandse Gemeenten en de Unie van Waterschappen zijn vertegenwoordigd. De Taskforce BID had als doel om het onderwerp informatieveiligheid gedurende twee jaar op de bestuurlijke agenda te zetten, om het bewustzijn van informatieveiligheid te vergroten. Ook was het doel om instrumenten te ontwikkelen om sturing op

[1] Onderzoeksraad voor de Veiligheid (2012), Het DigiNotarincident: waarom digitale veiligheid de bestuurstafel te weinig bereikt
[2] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging
[3] Eerste Kamer (2015), www.eerstekamer.nl
[4] Rekenkamer Den Haag (2014), Digitale Veiligheid
[5] FOX-IT (2015), Cybercriminelen hebben vrij spel
[6] Onderzoeksraad voor de Veiligheid (2012), Het DigiNotarincident: waarom digitale veiligheid de bestuurstafel te weinig bereikt

informatieveiligheid door bestuur en management mogelijk te maken.[7] Op 13 februari 2015 heeft de Taskforce BID haar coördinerende werkzaamheden beëindigd en zijn de betrokken (koepel)organisaties zelf verder gegaan met de ontwikkeling van informatieveiligheid.

De provincies en digitale informatieveiligheid

Reeds voor de oprichting van de Taskforce BID in 2013 richtten de provincies zich op het bevorderen van informatieveiligheid. Omdat provincies vergelijkbare werkprocessen hebben, streven zij onder het motto 'generiek waar het kan, specifiek waar het moet' zoveel mogelijk naar samenwerking op het terrein van informatieveiligheid.[8] Vanuit dit streven is het Centraal Informatiebeveiligingsoverleg (Cibo) opgericht, dat onderdeel is van het IPO. Het Cibo is een platform waarin provincies kennis en ervaring uitwisselen en de gezamenlijke ontwikkeling van informatieveiligheid vormgeven.[9] Vanuit elke provincie is een deelnemer vertegenwoordigd die werkzaam is op het gebied van informatieveiligheid. In 2010 heeft het Cibo, in samenwerking met het IPO, de Interprovinciale Baseline Informatiebeveiliging (IBI) opgesteld.[10] De IBI vormt het formele basisnormenkader voor provincies en bevat richtlijnen op het gebied van informatieveiligheid. Het doel is om provincies op een vergelijkbare manier te laten werken aan informatieveiligheid. De IBI geeft een standaard werkwijze waarmee per bedrijfsproces of informatiesysteem bepaald wordt welke beveiligingsmaatregelen getroffen moeten worden. Het principe van 'Verplichtende Zelfregulering' staat centraal. Dit betekent dat iedere provincie zelf verantwoordelijk is voor het informatieveiligheidsbeleid, met als stok achter de deur dat wanneer de informatieveiligheid onvoldoende wordt geïntegreerd in de bedrijfsvoering, verplichtingen op basis van (wettelijke) regelgeving zullen volgen.[11]

Op basis van de IBI heeft het Cibo een Agenda voor ontwikkeling informatieveiligheid provincies 2014 opgesteld.[12] Deze agenda is feitelijk een plan van aanpak, waarmee provincies de verplichtende zelfregulering kunnen implementeren. Om de informatieveiligheid van de provincies verder te optimaliseren en professionaliseren is het Convenant Interprovinciale Regulering Informatieveiligheid opgesteld, dat eind 2014 is ondertekend door alle provincies en op zowel ambtelijk als bestuurlijk niveau is vastgesteld.[13] Het convenant is een afsprakenkader waarmee provincies verantwoordelijkheid nemen voor het opstellen, uitvoeren en handhaven van het informatieveiligheidsbeleid. Het is de bedoeling dat de provincies op deze manier één standaard ontwikkelen en behouden waardoor informatieveiligheid geen vrijblijvend proces is. Het convenant helpt op deze manier de verplichtende zelfregulering te realiseren. Als het convenant echter tot onvoldoende verbetering leidt, dan blijft het mogelijk dat het Rijk regelgeving opstelt.

Concrete aanleidingen voor het onderzoek door de Randstedelijke Rekenkamer

De ondertekening van het convenant (november 2014) en de beëindiging van de werkzaamheden van de Taskforce BID (februari 2015) zijn voor de Randstedelijke Rekenkamer aanleiding om de informatieveiligheid van de vier Randstedelijke provincies te onderzoeken. Het is relevant in hoeverre het convenant daadwerkelijk is ingebed in de bestuurlijke, organisatorische en technische processen van de provincies. Een andere aanleiding is een onderzoek van de Rekenkamer Den Haag naar de digitale veiligheid van de ICT-infrastructuur en van privacygevoelige informatie bij de gemeente Den Haag in 2014.[14] De Rekenkamer Den Haag concludeerde dat

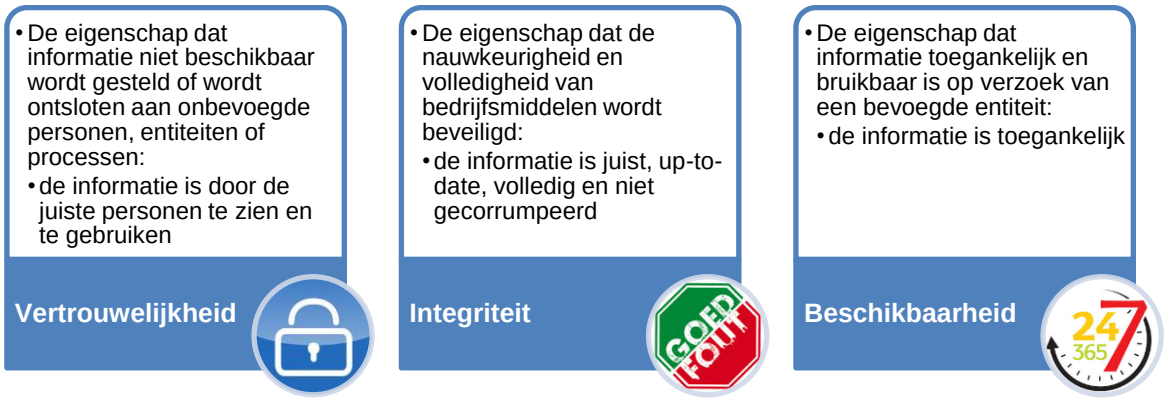
[7] Taskforce BID, http://www.taskforcebid.nl/faq/doelen-van-de-taskforce-bid/
[8] Cibo en IPO (2014), Convenant Interprovinciale Regulering Informatieveiligheid
[9] Cibo (2014), Agenda voor ontwikkeling informatieveiligheid provincies 2014
[10] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging
[11] Cibo (2014), Agenda voor ontwikkeling informatieveiligheid provincies 2014
[12] Cibo (2014), Agenda voor ontwikkeling informatieveiligheid provincies 2014
[13] Cibo en IPO (2014), Convenant Interprovinciale Regulering Informatieveiligheid
[14] Rekenkamer Den Haag (2014), Digitale Veiligheid

het zicht en de grip op informatieveiligheid door de gemeenteraad onvoldoende was. De gemeentelijke website bleek veilig te zijn. Maar op het interne netwerk werden de nodige kwetsbaarheden in de veiligheid gevonden en het bleek mogelijk op verschillende manieren van buiten toegang tot het interne netwerk te verkrijgen. De Rekenkamer Den Haag deed de aanbeveling om meer bestuurlijke aandacht te geven aan digitale veiligheid en periodiek integrale testen uit te voeren.

2. Achtergrond

De begrippen 'informatieveiligheid' en 'informatiebeveiliging' worden vaak simultaan gebruikt. Er is echter een verschil tussen beide begrippen: om informatieveiligheid (doel) te waarborgen, wordt gebruik gemaakt van informatiebeveiliging (maatregelen).[15] De Randstedelijke Rekenkamer kiest overwegend voor de term 'informatieveiligheid', omdat deze term in de perceptie meer recht doet aan de breedte van het onderwerp dan de term 'informatiebeveiliging', dat vaak wordt geassocieerd met ICT.

Informatieveiligheid richt zich op bescherming van informatie tegen dreigingen om de continuïteit van bedrijfsactiviteiten te waarborgen.[16][17] Indien de informatieveiligheid onvoldoende is gewaarborgd, kunnen er risico's ontstaan bij de uitvoering van provinciale taken en het functioneren van de organisatie. De maatregelen die genomen worden, moeten echter in verhouding staan tot de grootte van het risico. 100 procent veiligheid bestaat niet. Het doel van informatieveiligheid is daarom risico's tot een acceptabel niveau terug te brengen.[18] Informatieveiligheid heeft betrekking op het behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie (zie Figuur 2).[19][20]



Figuur 2 Aspecten van informatieveiligheid

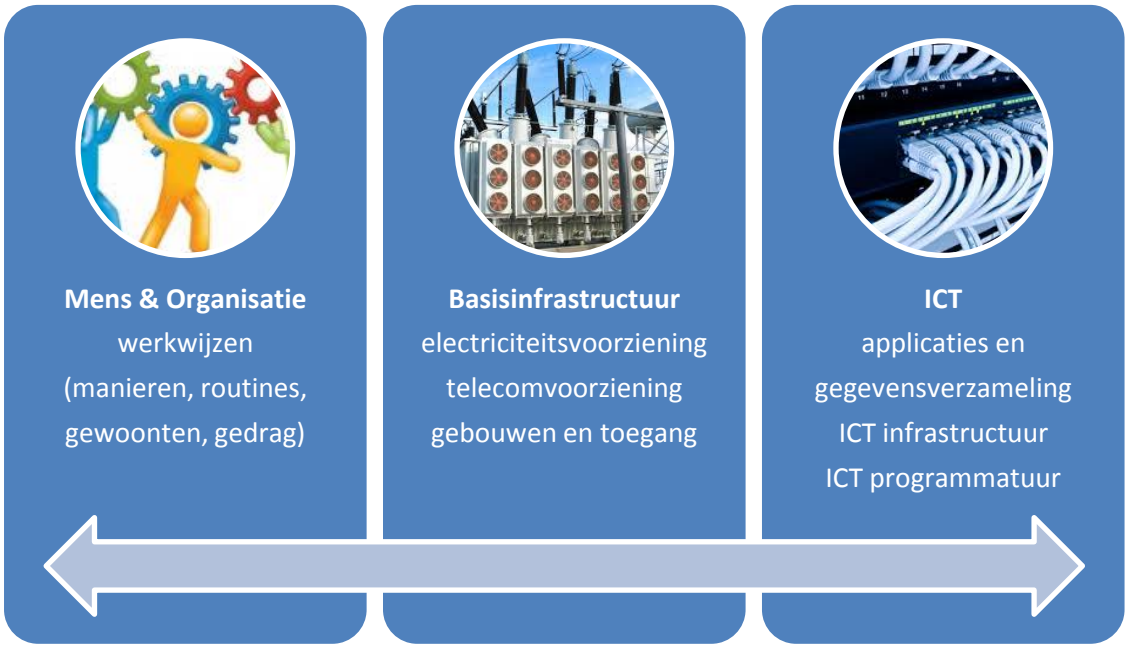
In Tabel 1 staan per aspect kenmerken genoemd die zorgen voor een hogere mate van informatieveiligheid en wat de bedreigingen zijn indien niet aan de kenmerken wordt voldaan, met enkele voorbeelden.

[15] Provincie Zuid-Holland (2014), Integraal veiligheidsbeleid provincie Zuid-Holland, Deel 2 Beleid Informatieveiligheid 2014-2018
[16] Provincie Noord-Holland (2012), Informatiebeveiligingsbeleid
[17] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging
[18] Taskforce BID, http://www.taskforcebid.nl/overheidslagen/provincies/
[19] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging, p. 4 (oorspronkelijke bron: NEN (2005), NEN-ISO/IEC-27001/27002)
[20] Provincie Noord-Holland (2012), Informatiebeveiligingsbeleid

Tabel 1 Informatieveiligheid: bedreigingen[21]

	Aspecten		
	Vertrouwelijkheid	**Integriteit**	**Beschikbaarheid**
Kenmerk	Exclusiviteit	1. Correctheid 2. Volledigheid 3. Geldigheid 4. Authenticiteit 5. Onweerlegbaarheid	1. Tijdigheid 2. Continuïteit
Bedreiging	Onthulling Misbruik	1. Wijziging 2. Verwijdering/Toevoeging 3. Veroudering 4. Vervalsing 5. Verloochening	1. Vertraging 2. Uitval
Voorbeeld	Afluisteren van netwerk Hacking	1. Onrechtmatig wijzigen 2. Onrechtmatige verwijdering / Toevoeging 3. Gegevens niet up-to-date 4. Frauduleuze transactie 5. Ontkennen berichten te hebben verstuurd	1. Overbelasting infrastructuur 2. Defect in infrastructuur

Om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te behouden en/of te vergroten, zijn er verschillende aandachtsgebieden waarop kan worden gestuurd en waar maatregelen kunnen worden genomen. Het gaat daarbij om drie aandachtsgebieden (zie Figuur 3).[22]



Figuur 3 Aandachtsgebieden van informatieveiligheid

[21] Provincie Zuid-Holland (2014), Integraal veiligheidsbeleid, Deel 2: Beleid Informatieveiligheid 2014-2018, p.5
[22] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging, p. 5

Tabel 2 geeft voor elk van de aandachtsgebieden een aantal voorbeelden weer van maatregelen die genomen kunnen worden om de verschillende aspecten van informatieveiligheid te bereiken en te waarborgen.

Tabel 2 Informatieveiligheid: aspecten- en aandachtsgebiedenmatrix met voorbeelden

		Aspecten		
		Vertrouwelijkheid	**Integriteit**	**Beschikbaarheid**
Aandachtsgebieden	**Mens & Organisatie**	Creëren van bewustzijn Procedures (o.a. voorschriften voor wachtwoorden, uitloggen bij inactiviteit, etc.)	Creëren van bewustzijn Procedures (o.a. functiescheiding)	Creëren van bewustzijn Procedures (o.a. beleggen van verantwoordelijkheid voor bijv. back-up en uitwijksystemen)
	Basis-infrastructuur	Toegangsbeveiliging gebouwen en ruimtes	Toegangsbeveiliging gebouwen en ruimtes	Noodstroomvoorziening
	ICT	Autorisatierechten (o.a. *role-based access*[23])	Autorisatierechten (o.a. RBAC) Logfiles bijhouden	Opstellen reserveapparatuur Installeren antivirusprogramma

3. Probleemstelling en onderzoeksvragen

De Randstedelijke Rekenkamer heeft voor dit onderzoek de volgende doel- en vraagstelling geformuleerd.

Doelstelling
Het doel van dit onderzoek is om inzichtelijk te maken of de informatieveiligheid van de provincie voldoende is geborgd. De uitkomsten van het onderzoek zullen we gebruiken om PS en GS handvatten te bieden voor het verbeteren van de informatieveiligheid.

Vraagstelling
Heeft de provincie de informatieveiligheid voldoende geborgd?

De vraagstelling wordt beantwoord aan de hand van een aantal onderzoeksvragen. Er zijn vier onderzoeksvragen, waarbij onderzoeksvraag 2 in drie delen is gesplitst.

1. Heeft de provincie de *sturing* op en de *verantwoordelijkheid* voor informatieveiligheid goed verankerd?
2. Is het informatieveiligheidsbeleid in opzet, uitvoering én in resultaat adequaat?
   a. Heeft de provincie een informatieveiligheidsbeleid opgesteld dat voldoet aan de gestelde eisen?
   b. Voert de provincie de benodigde[24] informatieveiligheidsmaatregelen uit?
   c. Is informatie in de praktijk voldoende beschermd tegen toegang door onbevoegden?[25]

[23] *Role-based access* (RBAC) houdt in dat een medewerker alleen toegang heeft tot die informatie en systemen waar hij/zij vanwege zijn/haar rol in de organisatie toegang tot moet hebben. Kenmerk van RBAC is dat individuen niet rechtstreeks worden geautoriseerd in informatiesystemen, maar dat ze uitsluitend rechten krijgen door een vorm van groepslidmaatschap, op basis van de rol die ze hebben binnen een organisatie of bedrijfsproces. Ook de permissies op objecten/functies in informatiesystemen kunnen worden gegroepeerd in rollen. Door het koppelen van de rol van de gebruiker in de organisatie aan een rol in een informatiesysteem, is het eenvoudig om de effectieve rechten van een gebruiker te bepalen.

[24] 'Benodigd' betekent: alle maatregelen uit de door de provincies onderschreven Interprovinciale Baseline Informatiebeveiliging die als generiek zijn gecategoriseerd en die daarmee het basisniveau aangeeft waaraan elke provincie moet voldoen en alle aanvullende maatregelen die de individuele provincie zelf heeft geclassificeerd als 'nodig', op basis van de door de provincie uitgevoerde risicoanalyse.

3. Heeft de provincie voldoende aandacht voor bewustwording op het gebied van informatieveiligheid?
4. Heeft de provincie het afleggen van verantwoording over en het houden van toezicht op informatieveiligheid goed geregeld?

De wijze waarop de onderzoeksvragen zullen worden beantwoord, komt aan bod in paragraaf 6 Werkwijze.

4. Afbakening

In paragraaf 2 kwam naar voren dat informatieveiligheid een breed en complex begrip is. Informatieveiligheid heeft betrekking op het behouden van de aspecten vertrouwelijkheid, integriteit en beschikbaarheid van informatie, waarbij onderscheid kan worden gemaakt tussen digitale en fysieke informatieveiligheid. Daarnaast kunnen maatregelen worden genomen op de aandachtsgebieden mens & organisatie, basisinfrastructuur en ICT, om de informatieveiligheid te vergroten.

Dit onderzoek richt zich op informatieveiligheid in de breedte. Uitzondering hierop vormt onderzoeksvraag 2c. Deze vraag, bestaande uit een toets van de daadwerkelijke informatieveiligheid, richt zich specifiek op het aspect van vertrouwelijkheid binnen het aandachtsgebied ICT.

5. Beoordelingskader

De Rekenkamer hanteert voor het maken van haar bevindingen een beoordelingskader. Het beoordelingskader is gebaseerd op o.a. de volgende bronnen:

- Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging
- Cibo en IPO (2014), Convenant Interprovinciale Regulering Informatieveiligheid
- Expertinterviews en vakliteratuur

In de Interprovinciale Baseline Informatiebeveiliging (IBI) en het Convenant Interprovinciale Regulering Informatieveiligheid, dat door alle provincies is ondertekend, staat het principe van verplichtende zelfregulering centraal. In een zelfregulerend besturingsmodel zijn vier kernaspecten te onderscheiden[26], waarop de onderzoeksvragen zijn gebaseerd. Deze worden hieronder kort toegelicht.

Het eerste kernaspect is ‘sturing en verantwoordelijkheid’. Naast de ICT infrastructuur horen zaken als toegangsbeveiliging, personeel en beleid tot het werkgebied van informatieveiligheid. Hierdoor kan informatieveiligheid niet de verantwoordelijkheid van één directie of afdeling zijn. Het is daarom van belang dat de provincie de sturing op en verantwoordelijkheid voor informatieveiligheid goed heeft verankerd.

Het tweede kernaspect is ‘beleid en normenkader’. De IBI is het vastgestelde basisnormenkader voor provincies, op basis waarvan de provincies een eigen informatieveiligheidsbeleid formuleren. Het tweede kernaspect is in drie onderzoeksvragen gesplitst en richt zich op de ‘opzet’ (2a), de ‘uitvoering’ (2b) en het ‘resultaat’ (2c) van het informatieveiligheidsbeleid. Vraag 2a gaat na of de provincie een informatieveiligheidsbeleid heeft geformuleerd, dat is gebaseerd op de IBI en daaruit volgende eisen. Vraag 2b richt zich vervolgens op de uitvoering van het

[25] Deze deelvraag richt zich op het aspect vertrouwelijkheid binnen het aandachtsgebied ICT.
[26] Cibo en IPO (2014), Convenant Interprovinciale Regulering Informatieveiligheid

beleid en de benodigde maatregelen, waarbij onderscheid wordt gemaakt tussen generieke en aanvullende maatregelen (op basis van een eigen provincie-specifieke risicoanalyse en –afweging geselecteerde) .[27] Dit zegt echter nog niets over de daadwerkelijke veiligheid van informatie: bieden de genomen maatregelen voldoende waarborgen tegen oneigenlijke toegang tot systemen en bestanden? Vraag 2c betreft daarom een toets op het resultaat van het informatieveiligheidsbeleid en de uitvoering van de maatregelen daarvoor. Hieruit zal blijken of aanpassingen in het informatieveiligheidsbeleid en/of maatregelen nodig zijn.

Het derde kernaspect is 'bewustwording, kennis en coördinatie'. Door aandacht te besteden aan leren, stimuleren en kennisdelen wordt de bewustwording van bestuur, management en medewerkers met betrekking tot informatieveiligheid vergroot. Bij de derde onderzoeksvraag wordt nagegaan of de provincie voldoende aandacht besteedt aan bewustwording op het gebied van informatieveiligheid.

Het laatste kernaspect is 'verantwoording en toezicht'. Dit omvat het verankeren van informatieveiligheid in de reguliere planning en control cyclus, het periodiek uitvoeren van een onafhankelijke toets en zelfevaluaties en de rol van PS. De laatste onderzoeksvraag gaat na of de provincie het afleggen van verantwoording en het houden van toezicht op informatieveiligheid goed heeft geregeld.

Aangezien de onderzoeksvragen zijn gebaseerd op deze vier kernaspecten, zal ook het beoordelingskader hier in belangrijke mate op steunen. De Rekenkamer zal het concept beoordelingskader bespreken met ambtelijke vertegenwoordigers van de vier provincies. Mede op basis van inzichten uit deze bespreking wordt het beoordelingskader voor het onderzoek definitief gemaakt.

6. Werkwijze

Deze paragraaf beschrijft op welke wijze de beantwoording van de onderzoeksvragen plaatsvindt. Het onderzoek wordt in alle vier de provincies uitgevoerd. Voor het beantwoorden van de onderzoeksvragen worden interviews gehouden met de ambtelijke organisatie en relevante documenten bestudeerd.

Voor de beantwoording van vraag 1 zal o.a. worden nagegaan of en in welke documenten verantwoordelijkheden, taken en bevoegdheden zijn toegekend aan de verschillende functies binnen de organisatie. Voor vraag 2 zal het beleidskader informatieveiligheid worden geanalyseerd (2a) en vervolgens de uitvoering van de maatregelen in kaart worden gebracht (2b). Voor het beantwoorden van onderzoeksvraag 2c worden de technische waarborgen voor het beschermen van informatie voor toegang door onbevoegden door een externe partij onderzocht. Aangezien de provincie Nood-Holland recentelijk (september 2015) met een nieuwe contractpartij voor de hosting van (kantoor)automatisering is gestart, zal de praktijktoets – gelet op de mogelijke impact en de risico's van deze praktijktoets – niet in deze provincie worden uitgevoerd. Vraag 3 vergt een analyse van (de uitvoering van) het bewustwordingsprogramma en alle andere activiteiten die eventueel worden ondernomen om bewustwording van informatieveiligheid te bevorderen. Voor de beantwoording van vraag 4 wordt nagegaan of informatieveiligheid een plek heeft in de P&C-documenten en of een onafhankelijke toets en zelfevaluatie worden uitgevoerd. Het eindrapport zal tevens op een aantal onderdelen een provincievergelijking bevatten.

[27] Benodigde maatregelen zijn in ieder geval de generieke maatregelen uit de IBI en daarnaast aanvullende maatregelen op basis van de eigen risicoanalyse van de provincie en de interprovinciale monitoringtool.

7. Organisatie, rapportage, planning & procedure

Organisatie

Dit onderzoek zal worden uitgevoerd door:

- dr. Jeroen van den Heuvel (projectleider);
- dr. Annalies Teernstra (onderzoeker);
- drs. Dharma Tjiam (onderzoeker).

Rapportage, planning & procedure

In Tabel 3 is een planning op hoofdlijnen opgenomen voor het opstellen van het rapport. In overleg met de contactpersonen per provincie zal de uitvoering van het onderzoek nader worden afgestemd. Dit geldt in het bijzonder voor het provinciespecifieke deel van het onderzoek.

Tabel 3 Planning onderzoek

Fase	Planning	Product
Vooronderzoek	juli – september	Onderzoeksopzet
Onderzoek	oktober – december	Concept Nota van bevindingen
Wederhoor, feitelijk	Januari	Nota van bevindingen
Wederhoor, bestuurlijk	februari 2016	Bestuurlijke nota
Publicatie	maart 2016	Eindrapport + 5 minutenversie
Behandeling	voorjaar 2016	Presentatie + behandeling

De Rekenkamer stelt een rapport op waarin de bevindingen staan uitgeschreven. Deze concept Nota van bevindingen zal bij de provincie worden voorgelegd voor feitelijk wederhoor. Na ontvangst van de reactie op het feitelijk wederhoor wordt de concept Bestuurlijke nota opgesteld. Deze nota bevat de conclusies en aanbevelingen, inclusief een provincievergelijking. De concept Bestuurlijke nota zal worden voorgelegd voor bestuurlijk wederhoor. Voorafgaand aan het bestuurlijk wederhoor kan over de resultaten van het onderzoek een gesprek plaatsvinden met de verantwoordelijk gedeputeerde. De Bestuurlijke nota, de reactie van GS en het nawoord van de Randstedelijke Rekenkamer vormen samen het eindrapport. Dit rapport en een 5 minutenversie van het onderzoek zullen in het voorjaar van 2016 behandeld kunnen worden door PS.

8. Slotopmerkingen

- Deze onderzoeksopzet is opgesteld op basis van een globale verkenning van het onderwerp. Op basis van het verzamelde onderzoeksmateriaal en voortschrijdend inzicht, kan de aanpak gedurende het onderzoek worden bijgesteld. Indien dit naar het oordeel van de Randstedelijke Rekenkamer tot majeure aanpassingen van de opzet leidt, wordt dit schriftelijk kenbaar gemaakt.
- De Randstedelijke Rekenkamer deelt aan PS en GS alle opmerkingen en bedenkingen mee die zij naar aanleiding van haar bevindingen van belang acht. Ook als dit niet expliciet onderdeel is van de onderzoeksopzet.
- Voor de uitvoering van het onderzoek is het van belang dat wij inzage hebben in alle relevante stukken waarover de provincie beschikt.

Colofon

RANDSTEDELIJKE REKENKAMER

Randstedelijke Rekenkamer
Teleportboulevard 110
1043 EJ Amsterdam

020 – 581 85 85 TELEFOON
info@randstedelijke-rekenkamer.nl EMAIL
www.randstedelijke-rekenkamer.nl INTERNET

Amsterdam
September 2015