Nota van bevindingen Informatieveiligheid

van de
rekenkamercommissie van het
hoogheemraadschap van Rijnland

20 september 2017
RC17.004

Hoogheemraadschap van

Rijnland

Inhoud

1	Algemeen	4
1.1	Achtergrond en aanleiding	4
1.2	Doelstelling en scope	4
1.3	Planning	4
1.4	Aanpak	5
2	Bevindingen	6
2.1	Opvolging adviezen Taskforce BID	6
2.2	Beleid en organisatie	9
2.3	Risicoanalyse	11
2.4	Cyclus van informatieveiligheid	13
2.5	Beveiligingsincidenten	14

1 Algemeen

1.1 Achtergrond en aanleiding

De rekenkamercommissie (RKC) van het hoogheemraadschap van Rijnland heeft als taak en doel om de VV te ondersteunen bij de kaderstellende en controlerende rol van dit algemeen bestuur. Voor VV leden is het belangrijk zicht te hebben op hoe Rijnland omgaat met informatieveiligheid en met de risico's die zij loopt, zowel technisch als bestuurlijk.

VV leden hoeven zeker geen informatieveiligheidsspecialist te zijn om deze verantwoordelijkheid goed uit te kunnen voeren. Het gaat er immers niet om dat de VV weet hoe de organisatie informatieveiligheid tot in de details borgt, het gaat er vooral om dat de VV weet dat het wordt geborgd en dat het college een stuur zet op het onderwerp en kan bijsturen waar nodig. Om de VV hierbij te ondersteunen heeft de RKC besloten een onderzoek in te stellen naar beleid en uitvoeringspraktijk van Rijnland op het gebied van informatieveiligheid en privacybescherming.

1.2 Doelstelling en scope

De centrale onderzoeksvraag voor dit onderzoek luidt als volgt: *Is Rijnland 'in control' als het om informatieveiligheid en privacybescherming gaat?*

De beantwoording van deze centrale onderzoeksvraag valt uiteen in de volgende onderzoeksvragen:

1. Hoe heeft het college uitvoering gegeven aan de adviezen van de Taskforce BID, zoals die specifiek voor waterschappen gegeven zijn?
2. Hoe is het informatiebeveiligingsbeleid vormgegeven binnen het waterschap? Wie zijn er als verantwoordelijken aangesteld en is er aandacht voor bewustwording?
3. Welke risico's accepteert het college en welke niet? Welke politiek-bestuurlijke en maatschappelijke gevolgen kan dit hebben in geval van een incident? Is de privacy van de burgers, bedrijven en overige belanghebbenden gegarandeerd? Ook in relatie tot verbonden partijen?
4. Functioneert de cyclus van informatieveiligheid binnen het waterschap? Vindt er een jaarlijkse toetsing plaats om na te gaan of het waterschap in control is op het gebied van informatieveiligheid via peer reviews, audits of self-assessment? Wat zijn de resultaten van deze toetsing? Wordt de cyclus jaarlijks bijgesteld op basis van lessons learned?
5. Zijn er binnen het waterschap procedures opgesteld voor incidenten? Welke risico's loopt Rijnland in geval van verstoring of cyberaanval, ook wanneer deze verstoring elders in de keten plaatsvindt? Hoeveel incidenten zijn er in de afgelopen periode (maand/half jaar) geweest? Meldt Rijnland die incidenten bij de IBD?

Het beoogde resultaat is een praktische beoordeling van beleid en uitvoeringspraktijk, voorzien van concrete aanbevelingen.

1.3 Planning

Het onderzoek is uitgevoerd in de periode juli – augustus 2017. In september 2017 is het ambtelijk wederhoor uitgevoerd, waarbij de SAD in de gelegenheid is gesteld om de concept nota van bevindingen te controleren op feitelijke onjuistheden. De ambtelijke reactie is ontvangen op 18 september 2017 waarna de rekenkamercommissie de nota van bevindingen heeft vastgesteld (en de wijze van verwerking door middel van een separate notitie heeft toegelicht aan de SAD).
Teneinde de toegankelijkheid van de nota van bevindingen te vergroten heeft de rekenkamercommissie de beantwoording van de deelvragen voorzien van een 'stoplichtmodel', waardoor de nuances in het onderzoek beter tot uitdrukking komt.
In september 2017 is het bestuurlijk wederhoor uitgevoerd.
In de VV van 8 november 2017 wordt het resultaat gepresenteerd.

1.4 Aanpak

Om de onderzoeksvragen te beantwoorden heeft de RKC gekozen voor een beleidsmatig en een technisch onderzoek. Hieronder wordt de aanpak van beide onderzoeken beschreven. Om de onderzoeksvragen voor het beleidsonderzoek te beantwoorden zijn de volgende activiteiten uitgevoerd:

1. Interviews met:
    a. Ronald Marseille;
    b. Peter Waij;
    c. Albert van As;
    d. Linda van Mourik;
    e. Luc van Wijk;
    f. Pieter van Dijk;
    g. Wim Breugom;

    Van alle interviews is een beperkte vastlegging gemaakt die door geïnterviewden zijn geaccordeerd.
2. Bestuderen documentatie met betrekking tot:
    a. Beleidsdocumenten inzake informatieveiligheid;
    b. Projectdocumentatie inzake implementatie BIWA en AVG;
    c. Overeenkomsten inzake gemeenschappelijke regeling BSGR;
    d. Beschikbare procedures inzake informatieveiligheid;
    e. Registratie van beveiligingsincidenten;
    f. Organisatiestructuur inzake informatieveiligheid;
    g. Planningscyclus inzake informatieveiligheid;
    h. Bewustwordingsproces inzake informatiebeveiliging;
3. Kennis genomen van:
    a. Overeenkomsten met dienstverleners, met name inzake de bepalingen over privacy en informatieveiligheid;
    b. Eerdere uitgevoerde externe onderzoeken.

Het technisch onderzoek is als volgt uitgevoerd:

1. Extern onderzoek:
    a. Openbronnenonderzoek om in kaart te brengen welke systemen beschikbaar zijn vanaf het internet;
    b. Hertest van gevonden kwetsbaarheden naar aanleiding van reeds uitgevoerd beveiligingsassessment;
    c. Uitvoeren van externe scans op kwetsbaarheden;
    d. Analyseren van kwetsbaarheden;
2. Intern onderzoek (uitgevoerd op locatie):
    a. In kaart brengen van het interne netwerk;
    b. Analyse WiFi-netwerken;
    c. Uitvoeren van scans op kwetsbaarheden;
    d. Analyseren van kwetsbaarheden.

Het technisch onderzoek was beperkt tot de systemen van Rijnland.

2 Bevindingen

De bevindingen zijn hieronder beschreven als antwoorden op de in paragraaf 1.2 geformuleerde deelvragen.

2.1 Opvolging adviezen Taskforce BID

Deelvragen	Status	Toelichting
Het opstellen en vaststellen van een beleidsplan informatieveiligheid met doelen, maatregelen en budget		Bestaat, op het budgetcomponent na
Het in de begroting opnemen van het benodigde budget om informatieveiligheid adequaat in te kunnen richten		Afwezig vanaf 2017, daarvoor als projectbudget gedefinieerd
De implementatie van de Baseline Informatiebeveiliging Waterschappen (BIWA)		HHR heeft een aanzet gemaakt tot de implementatie van de BIWA
Het inrichten van een PDCA-cyclus informatieveiligheid als onderdeel van de reguliere Planning & Control-cyclus		Ingericht vanaf 2017
Het meten van informatieveiligheid aan de hand van indicatoren		1 rapportage gezien
Het aanleveren van de meting naar de koepel (UvW) ten behoeve van een beeld over de overheidslaag heen		1 aangeleverde meting gezien
Het treffen van voorbereidingen voor een audit op informatieveiligheid		Afwezig, alleen globaal gepland
Het inrichten van incidentregistratie en incidentrapportages		Formele procedure afwezig, incidentenregister bestaat

Uitleg kleuren:
Groen = opzet en bestaan vastgesteld
Oranje = opzet en bestaan deels vastgesteld
Rood = opzet en bestaan afwezig

Bevindingen
Van 2013 tot 2015 heeft de minister van BZK een Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) ingesteld met als doel ‘bestuurders te doordringen van het belang van digitale veiligheid’ en ‘hen te voorzien van voldoende inzicht en vaardigheden om hen in staat te stellen actief sturing te geven aan de beheersing van digitale veiligheid in hun organisatie’, verplichtende zelfregulering genoemd.
Bij de instelling van de Taskforce BID hebben het Rijk en de medeoverheden zich gecommitteerd aan het principe van de verplichtende zelfregulering (pagina 5 van de eindrapportage BID). In februari 2015 is de eindrapportage van de Taskforce BID opgeleverd met daarin diverse adviezen voor overheden om het principe van verplichtende zelfregulering te kunnen inrichten. De adviezen van de Taskforce BID (pagina 37 van de eindrapportage BID, onder kopje Verankering Waterschappen) zijn hieronder puntsgewijs opgesomd:

1. Het opstellen en vaststellen van een beleidsplan informatieveiligheid met doelen, maatregelen en budget;
2. Het in de begroting opnemen van het benodigde budget om informatieveiligheid adequaat in te kunnen richten;
3. De implementatie van de Baseline Informatiebeveiliging Waterschappen (BIWA). De BIWA is opgesteld door, wordt onderhouden door en is vastgesteld door de Unie van

Waterschappen en biedt een standaard set van maatregelen die algemeen voorkomende informatiebeveiligingsrisico's bij waterschappen afdekken. De BIWA is geen wettelijke verplichting maar met de instelling van de Taskforce BID hebben alle waterschappen zich gecommitteerd aan het principe van verplichtende zelfregulering en daarmee de implementatie van de BIWA;

4. Het inrichten van een PDCA-cyclus informatieveiligheid als onderdeel van de reguliere P&C-cyclus;
5. Het meten van informatieveiligheid aan de hand van indicatoren;
6. Het aanleveren van de meting naar de koepel (UvW) ten behoeve van een beeld over de overheidslaag heen;
7. Het treffen van voorbereidingen voor een audit op informatieveiligheid;
8. Het inrichten van incidentregistratie en incidentrapportages.

De bevindingen van het onderzoek bij Rijnland zijn hieronder per advies van de Taskforce BID genoteerd. Een aantal van deze adviezen komen ook in detail terug in andere deelvragen, in dat geval wordt verwezen naar deze deelvraag.

2.1.1 *Het opstellen en vaststellen van een beleidsplan informatieveiligheid met doelen, maatregelen en budget*

Ten aanzien van het informatiebeveiligingsbeleid is de CIO beleidsvoorbereidend en het directieteam stelt dit beleid vervolgens vast. Wij hebben vastgesteld dat de VV hier op 30 april 2014 over geïnformeerd is (zie Corsanummers 14.00687 en 14.00845). Het beleid wordt minimaal één keer in de drie jaar geëvalueerd en indien nodig bijgesteld.

Het opstellen van het informatiebeveiligingsplan gebeurt bottom-up. De afdelingshoofden leveren aan de CIO deelplannen op die door de CIO worden geconsolideerd. Deze consolidatie wordt vervolgens aan het directieteam voorgelegd. Het informatiebeveiligingsplan wordt jaarlijks door de directie vastgesteld.

Rijnland beschikt over een vastgesteld informatiebeveiligingsbeleid (september 2016) en -plan (juni 2017) met daarin doelen en te treffen maatregelen voor 2017. Budgettering van de te treffen maatregelen is niet opgenomen in het plan. In de ambtelijke reactie is aangegeven dat de budgettering verloopt via de reguliere P&C cyclus met afdelings-exploitatiebudgetten en investeringskredieten.

2.1.2 *Het in de begroting opnemen van het benodigde budget om informatieveiligheid adequaat in te kunnen richten*

Van 2014 tot 2016 is een project om de BIWA te implementeren uitgevoerd. 1 januari 2017 is dit project afgerond met de overdracht naar maatregeleigenaren. Maatregeleigenaren zijn verantwoordelijken voor de implementatie van de betreffende maatregel, vaak afdelingshoofden of teamleiders. Vanaf dat moment is geen separaat budget in de begroting meer opgenomen voor informatieveiligheid, maar valt dit onder de budgetten van de verschillende afdelingen. Dit project heeft niet geleid tot een adequate informatiebeveiliging, hiervoor verwijzen wij naar de hieronder volgende beleidsmatige en technische bevindingen.

2.1.3 *De implementatie van de BIWA*

Rijnland is sinds 2012 bezig met informatiebeveiliging. In 2012 is een project gestart Informatiebeveiliging en Bedrijfscontinuïteit (IBBC) met behulp van externe partij VKA.

Het project IBBC is later omgezet in de implementatie van de BIWA. De gehanteerde projectmethodiek is "Projectmatig creëren".

De implementatie van de BIWA is gestart met een risicoanalyse over alle gedefinieerde maatregelen van de BIWA (hoofdstuk 5 tot en met 15 van het strategisch en tactisch normenkader van de BIWA). Hierbij hebben diverse externe partijen ondersteund, waaronder InspearIT en Deloitte. De

risicoanalyse is volgens de Adviseur Informatievoorziening opgesteld door middel van workshops met informatieadviseurs op basis van professional judgment / common sense en is gevalideerd bij de uitvoerend verantwoordelijken. De bevindingen met betrekking tot het uitvoeren van de risicoanalyse worden beschreven in paragraaf 2.3.

De hierboven genoemde risicoanalyse vormde het startpunt voor de implementatie. Op basis hiervan is Rijnland medio 2015 begonnen met het implementeren van maatregelen met een hoge (risico) classificatie. In 2016 is hier vervolg aan gegeven middels de uitvoering van het informatiebeveiligingsplan. De toetsing en voortgang werden tijdens dit project uitgevoerd door de security board. Vanaf 1 januari 2017 is deze rol overgenomen door de i-Raad. De i-Raad is een samenwerking tussen Rijnland en hoogheemraadschap van Schieland en de Krimpenerwaard (hierna: HHSK) en heeft als hoofddoel toezicht te houden op respectievelijk aansturen van de gezamenlijke I&A afdeling die sinds 1 januari 2017 is opgericht.

Het project implementatie van de BIWA is 1 januari 2017 afgerond met de overdracht van maatregelen naar maatregeleigenaren, waarmee alle maatregelen belegd zijn in de organisatie. Op basis van het meest actuele statusoverzicht (‘actielijst BIWA-implementatie HHR 1.08’, ongedateerd) werkte een deel van de maatregelen inzake beleid. Veel van de maatregelen hebben in het meest actuele statusoverzicht nog de status Plan, wat wil zeggen dat deze nog volledig geïmplementeerd moeten worden. De implementatie van de BIWA is nog lang niet afgerond.

2.1.4 *Het inrichten van een PDCA-cyclus informatieveiligheid als onderdeel van de reguliere P&C-cyclus*

We hebben vastgesteld dat de inrichting van de Plan, Do, Check, Act (PDCA)-cyclus heeft plaatsgevonden. Met een PDCA-cyclus wordt een continu proces bedoeld waarmee informatiebeveiliging wordt gepland, geïmplementeerd, gecontroleerd en bijgestuurd. Hiermee wordt formeel voldaan aan het advies van de Taskforce BID. Voor bevindingen inzake het functioneren van de cyclus, zie paragraaf 2.4.

2.1.5 *Het meten van informatieveiligheid aan de hand van indicatoren*

Rijnland heeft zelf circa 40 Key Performance Indicatoren (KPI) op het gebied van informatieveiligheid opgesteld. De indicatoren zijn vastgesteld door de i-Raad. De rapportage over Q1 2017 is aanwezig. Dit is de eerste rapportage. De rapportage zal per kwartaal worden opgesteld door de CISO en wordt besproken in de i-Raad. Hiermee wordt formeel voldaan aan het advies.

2.1.6 *Het aanleveren van de meting naar de koepel (UvW) ten behoeve van een beeld over de overheidslaag heen*

Rijnland heeft over 2016 de meting naar de koepel (Unie van Waterschappen) aangeleverd. Hiermee wordt formeel voldaan aan het advies.

2.1.7 *Het treffen van voorbereidingen voor een audit op informatieveiligheid*

Jaarlijks wordt een (verplichte) audit uitgevoerd op de DIGID-aansluiting en voert de externe accountant een IT-audit uit in het kader van de controle op de jaarrekening (wat geen vervanging is van een audit op de informatieveiligheid. Tot op heden is nog geen audit op informatieveiligheid door Rijnland uitgevoerd (zowel niet intern als extern). In het najaar van 2017 staat volgens de CIO een externe audit namens de Unie van Waterschappen gepland (concrete planning moet nog worden gemaakt). De interne audit zal volgens de CISO niet eerder plaatsvinden dan Q4 van 2017. Voor beide audits zijn geen voorbereidingen voor aangetroffen.

2.1.8 *Het inrichten van incidentregistratie en incidentrapportages*

Rijnland heeft een incident management proces maar dit is gericht op verstoringen van de operatie (conform ITIL, een standaard best practice raamwerk voor beheersing van IT processen) en bevat geen aspecten die relevant zijn voor informatiebeveiligingsincidenten zoals mogelijke melding naar Autoriteit Persoonsgegevens of aangifte bij de politie.

Voor de vastlegging van informatiebeveiligingsincidenten heeft Rijnland een register waarin ook de afhandeling van incidenten wordt vastgelegd. Dit register wordt besproken in de i-Raad. De voeding van het register is onduidelijk. Klaarblijkelijk kan dit komen uit de hierboven vermelde ITIL procedure. Er is geen sprake van een formele vastlegging van de inrichting van de incidentregistratie. In het kader van de Algemene Verordening Gegevensbescherming (AVG) is Rijnland bezig met het ontwikkelen van een procedure voor incidentregistratie.

Het register ten behoeve van de i-Raad is te beschouwen als een incidentrapportage. Verder heeft Rijnland een gedragscode waarin summier de melding van informatiebeveiligingsincidenten wordt beschreven. Deze gedragscode kan niet worden beschouwd worden als formele procedure waarin is vastgesteld wie wat doet wanneer en waarom in het kader van informatiebeveiligingsincidenten.

2.2 Beleid en organisatie

Deelvragen	Status	Toelichting
Hoe is het informatiebeveiligingsbeleid vormgegeven binnen het waterschap?		Beleid is vastgesteld aanwezig
Wie zijn er als verantwoordelijken aangesteld		Verantwoordelijken zijn belegd, niet alle rollen zijn voldoende bemenst
Is er aandacht voor bewustwording?		Bestaat, er is aandacht voor bewustwording

Uitleg kleuren:
Groen = opzet en bestaan vastgesteld
Oranje = opzet en bestaan deels vastgesteld
Rood = opzet en bestaan afwezig

Bevindingen
De antwoorden zijn per deelvraag genoteerd.

2.2.1 *Hoe is het informatiebeveiligingsbeleid vormgegeven binnen het waterschap?*

Ten aanzien van het informatiebeveiligingsbeleid is de CIO beleidsvoorbereidend en het directieteam stelt dit beleid vervolgens vast. De VV wordt hierover geïnformeerd. Het beleid wordt minimaal één keer in de drie jaar geëvalueerd en indien nodig bijgesteld. Rijnland beschikt over een vastgesteld informatiebeveiligingsbeleid (gezamenlijk met HHSK).

Het informatiebeveiligingsbeleid heeft als doel het borgen van de bedrijfszekerheid en de kwaliteit van de informatie binnen Rijnland en HHSK. Daartoe gebruikt Rijnland de vigerende wet- en regelgeving inzake informatiebeveiliging en de internationale normering inzake informatiebeveiliging (ISO27001), verder uitgewerkt in de BIWA.

Het informatiebeveiligingsbeleid geldt voor heel Rijnland en voor zowel de kantoor- als de procesautomatisering en stelt de kaders vast waarbinnen de organisatie en beheersing van informatiebeveiliging binnen Rijnland dienen te zijn opgezet. Het beleid is in september 2016 vastgesteld, op voorstel van de CIO. Het beleid wordt onderhouden door de CIO van Rijnland en HHSK.

2.2.1 *Wie zijn er als verantwoordelijken aangesteld?*

De verantwoordelijkheden rondom informatiebeveiliging zijn binnen Rijnland per functionaris of gremium als volgt belegd:

1. ***Dagelijks bestuur***: verantwoordelijke ten aanzien van de VV voor informatiebeveiliging;
2. ***Directie***: verantwoordelijke ten aanzien van het dagelijks bestuur voor informatiebeveiliging en het vaststellen van het informatiebeveiligingsbeleid en -plan;
3. ***CIO***: opstellen concept informatiebeveiligingsbeleid en verantwoordelijk voor organisatie van informatiebeveiliging;
4. ***Afdelingshoofd:*** verantwoordelijk voor de uitvoering van informatiebeveiliging binnen de eigen afdeling, invoeren, volgen en handhaven richtlijnen beleid, voorbeeldfunctie, opnemen benodigde maatregelen in informatiebeveiligingsplan, opstellen eisen, procedures en protocollen, doorvoeren verbeteracties, autoriseren medewerkers, bewustwording op eigen afdeling, afhandelen van vertrouwelijke beveiligingsincidenten, rapporteren over invoering en werking van informatiebeveiliging;
5. ***Eigenaar informatiesysteem / fysiek object:*** verantwoordelijk voor de veiligheid van systeem / object.

De toetsende rollen zijn als volgt belegd:

1. ***i-Raad (voorheen ingevuld door Security Board)***: vaststellen uitvoeringsrichtlijnen, bewaken implementatie en bewaken uitvoering conform uitvoeringsrichtlijnen. Rijnland en HHSK hebben een gezamenlijke i-Raad, een gremium van zowel Rijnland als HHSK dat bedoeld is als advies gevend orgaan voor beide directies inzake de gezamenlijke afdeling I&A. Toezicht houden en adviseren over bijsturing waar nodig op het gebied van informatiebeveiliging is een van de taken van de i-Raad. De i-Raad wordt voorgezeten door de CIO;
2. ***Security Officer (CISO):*** toetsen van beleid rondom informatiebeveiliging, monitoren en bijsturen, registreren en afhandelen van beveiligingsincidenten, volgens het beleid verantwoordelijk voor samenstellen van informatiebeveiligingsplan. In de praktijk wordt het plan opgesteld door de CIO;
3. ***Privacy Officer:*** toetsen op naleving van WBP (en later AVG), opstellen aanbevelingen voor betere bescherming van verwerking van persoonsgegevens, melden van incidenten aan Autoriteit Persoonsgegevens.

Als laatste onderkent Rijnland Adviseurs Informatievoorziening die verantwoordelijk zijn voor het ondersteunen van afdelingshoofden en leidinggevenden en het bevorderen van de bewustwording. De rol adviseur informatievoorziening bij de procesautomatisering is het afgelopen jaar niet ingevuld geweest. Sinds 1 september 2017 is deze functie door werving van een nieuwe medewerker weer ingevuld.

De bevinding is dat er diverse beleidsstukken zijn die onderling op ondergeschikte punten niet consistent zijn ten aanzien van verantwoordelijkheden en rolbeschrijvingen. Dit betreft:

1. De ongedateerde memo “*Rollen van informatiebeveiliging bij HHR en HHSK*”, verkregen van de CIO;
2. Het informatiebeveiligingsbeleid (paragraaf 5.1).

De rol van security officer is belegd bij de concern controller; de rol van privacy officer is belegd bij het afdelingshoofd Organisatie en Advies. De huidige security officer is sinds eind 2016 aangesteld, hiervoor was deze verantwoordelijkheid belegd bij het afdelingshoofd Dienstverlening, Voorzieningen en ICT DVI).
Voor de privacy officer is niet bekend hoeveel FTE hiervoor beschikbaar is, voor de security officer is dit 0,1 FTE.

De rol van security officer is nog in ontwikkeling. De rol wordt ingevuld vanaf 1 september 2016, door de huidige functionaris.

2.2.2 *Is er aandacht voor bewustwording?*

Ja, Rijnland heeft een communicatieplan opgesteld met als doel dat medewerkers, management en bestuur bewust en veilig omgaan met (vertrouwelijke) informatie. Hiertoe heeft Rijnland diverse initiatieven gestart om de bewustwording te vergroten, waaronder:

1. Op intranet zijn pagina's met betrekking tot bewustwording geplaatst;
2. Rijnland heeft een enquête iBewustzijn uitgezet. Resultaten van dit onderzoek zijn ons niet bekend;
3. Rijnland heeft in 2016 een extern onderzoek laten uitvoeren met 'phishing mail'. De aanbevelingen zijn binnen het team geprioriteerd. Niet alle resultaten met een hoge prioriteit zijn opgevolgd.

Uit het interview met de security officer blijkt dat hij het als een belangrijke taak ziet om de bewustwording te bevorderen. Hij begeleidt ook een stagiair die zich met dit onderwerp bezighoudt.

Verder is het vooral de taak van afdelingshoofden om informatiebeveiliging steeds terug te laten komen op de agenda bij afdelingsoverleggen. Uit de rolbeschrijvingen blijkt dat hier ook een belangrijke taak ligt voor de adviseurs informatievoorziening en de medewerkers informatiebeveiliging.

2.3 Risicoanalyse

Deelvragen	Status	Toelichting
Welke risico's accepteert het college en welke niet?		Door gebruik onjuiste methodiek is dit niet inzichtelijk
Welke politiek-bestuurlijke en maatschappelijke gevolgen kan dit hebben in geval van een incident?		Door ontbreken van inzicht in risico's niet te beantwoorden.
Is de privacy van de burgers, bedrijven en overige belanghebbenden gegarandeerd? Ook in relatie tot verbonden partijen?		Opzet, HHR heeft een project gestart om te voldoen aan de Algemene Verordening Gegevensbescherming (AVG). Het technisch onderzoek heeft aangetoond dat op dit moment de werking onvoldoende is. N.B. De onderzoekers zijn niet in de gelegenheid geweest om dit bij de BSGR te onderzoeken.

Uitleg kleuren:
Groen = opzet en bestaan vastgesteld
Oranje = opzet en bestaan deels vastgesteld
Rood = opzet en bestaan afwezig

Bevindingen
De antwoorden zijn per deelvraag genoteerd.

2.3.1 *Welke risico's accepteert het college en welke niet?*

In overleg met het managementteam heeft Rijnland ervoor gekozen een analyse uit te voeren tussen de BIWA bepalingen (baseline) en de aanwezige situatie; en een weging te hechten aan de bijbehorende risico's op maatregelenniveau.

De implementatie van een informatiebeveiligingsraamwerk (zoals de BIWA) dient, volgens de rekenkamercommissie, te starten met een risicoanalyse op het niveau van kritische bedrijfsprocessen en te beveiligen objecten.
De BIWA beschrijft in haar doelstelling (paragraaf 1.2) dat de BIWA maatregelen bevat die algemeen voorkomende informatiebeveiligingsrisico's bij de waterschappen afdekken; dat de baseline een

aantal minimale beveiligingsniveaus bevat waaraan een waterschap zou moeten willen voldoen; maar ook dat deze nog niet volledig is. Voor risico's die niet door de baseline zijn afgedekt dient het management van het waterschap aanvullende maatregelen vast te stellen. Daarnaast beschrijft de BIWA (paragraaf 2.3) als randvoorwaarde dat 'Risicomanagement het uitgangspunt is voor informatieveiligheid', met als nadere toelichting dat de baseline een basis beveiligingsniveau biedt en dat voor informatiesystemen dient te worden vastgesteld of de baseline voldoende is.

Een risicoanalyse begint met de inventarisatie van de objecten die beveiligd moeten worden, gevolgd door een kwetsbaarheidsanalyse per object. Op basis hiervan worden de risico's vastgesteld (kans x impact) en vervolgens de classificaties hoog, midden of laag. Op basis hiervan worden de te treffen maatregelen gedefinieerd en geïmplementeerd. Veelal gebruikt men hiervoor de TARA methodologie waarbij de risico's worden verzekerd (transfer), vermeden (avoid), gereduceerd (reduced) of geaccepteerd (accept).

Wij hebben niet kunnen vaststellen dat deze analyse op de beschreven manier is uitgevoerd.

Wel hebben wij vastgesteld dat op basis van de maatregelen van de BIWA risico's zijn gedefinieerd en geclassificeerd (met behulp van diverse externe partijen ondersteund, waaronder InspearIT en Deloitte). Dit roept twijfel op over de volledigheid van de risico's. Wij kunnen hierdoor geen uitspraak doen over welke risico's het college niet accepteert.
De vraagstelling gaat bij deze onderzoekvraag uit naar welke risico's door het college zijn geaccepteerd en welke niet. De voorliggende documenten geven hierover geen uitsluitsel. Het relevante document "BIWA maatregelenanalyse 2.1" (opgesteld door de Adviseur informatievoorziening met hulp van de hierboven genoemde externe adviseurs) geeft een groot aantal risico's, afgeleid van de maatregelen van de BIWA met de classificatie hoog, midden of laag. Men zou verwachten dat bij laag risico aangegeven is of dit wordt geaccepteerd of niet. Dit is niet op detailniveau gebeurd.

In het informatiebeveiligingsbeleid is als *richtlijn* beschreven: "*Lage risico's zijn acceptabel. Voor lage risico's wordt alleen geïnvesteerd in maatregelen waarvan de waarde aantoonbaar is gemaakt.".*
Voor alle risico's met classificering midden of hoog dienen maatregelen te worden getroffen. Dit is ook beschreven in het memo 'Risicoanalyse informatiebeveiliging en bedrijfscontinuiteit' dat in 2015 aan het college is voorgelegd en een analyse bevatte op BIWA maatregelniveau (resp. 10 hoog – 71 midden – 52 laag). In dit memo - dat volgens de rekenkamercommissie op relatief hoog abstractieniveau is geformuleerd- is gesteld dat lage risico's acceptabel zijn, zonder een koppeling te maken met specifieke objecten.

Als voorbeeld: een te beschermen object is een server. Uit het technisch onderzoek blijkt dat op meerdere servers nog (zeer) verouderde besturingssystemen draaien. De risico's die dat met zich meebrengt zijn niet benoemd in de door Rijnland uitgevoerde analyse.

2.3.2 *Welke politiek-bestuurlijke en maatschappelijke gevolgen kan dit hebben in geval van een incident?*

Door het ontbreken van inzicht in welke risico's het college accepteert, is deze vraag niet eenduidig door ons te beantwoorden. Het is algemeen bekend dat incidenten inzake informatiebeveiliging politiek-bestuurlijk kunnen leiden tot ernstige imagoschade, het aantasten van het vertrouwen in het waterschap en ultiem aftreden van politiek verantwoordelijken. Voor wat betreft de maatschappelijke gevolgen is de bedrijfszekere werking van de IT van (met name de procesautomatisering) het waterschap essentieel voor de veiligheid van de inwoners binnen Rijnland. Het technisch onderzoek heeft aangetoond dat hier onaanvaardbare risico's worden gelopen, zie paragraaf 2.5.2.

2.3.3 *Is de privacy van de burgers, bedrijven en overige belanghebbenden gegarandeerd? Ook in relatie tot verbonden partijen?*

Voor wat betreft privacy, betreft het hier gegevens over personen die relevant zijn voor enerzijds de personeelsadministratie en anderzijds de belastingheffing.

Voor wat betreft de personeelsadministratie zijn in ieder geval bewerkersovereenkomsten afgesloten met Plusport (Aquademie) en ADP (salarisadministratie), beide SaaS oplossingen. Het is op dit moment niet inzichtelijk voor welke applicaties en diensten bewerkersovereenkomsten afgesloten zouden moeten worden. Rijnland gaat een inventarisatie starten om in kaart te brengen waar persoonsgegevens worden verwerkt en wat daar de eventuele te treffen maatregelen zijn. Dit is de eerste stap in een project dat is gestart om te voldoen aan de Algemene Verordening Persoonsgegevens in mei 2018. Dit project wordt uitgevoerd conform de projectmethodiek IPM.

Wat betreft de belastingheffing: deze heeft Rijnland ondergebracht in een gemeenschappelijke regeling, de BSGR. Rijnland heeft met de BSGR een dienstverleningsovereenkomst afgesloten waarin de BSGR verklaart dat zij de nodige maatregelen zullen treffen om te voldoen aan relevante wet- en regelgeving, zoals de Wet Bescherming Persoonsgegevens (WBP). Daarnaast laat de BSGR jaarlijks diverse externe audits uitvoeren zoals een DigiD assessment en een ISAE3402 type I en type II audit, waaruit Rijnland informatie kan putten over het “in control” zijn van de BSGR.

Het stelsel van interne controle van Rijnland is essentieel voor de handhaving van de privacy. Het technisch onderzoek heeft aangetoond dat dat deze onvoldoende functioneert en dat hierdoor op dit moment de privacy bij Rijnland niet gegarandeerd is. De privacy bij de belastingheffing kon binnen dit onderzoek van de rekenkamercommissie bij de BSGR niet worden onderzocht.

2.4 Cyclus van informatieveiligheid

Deelvragen	Status	Toelichting
Functioneert de cyclus van informatieveiligheid binnen het waterschap?		Cyclus is opgezet in 2017, nog niet volledig uitgevoerd
Vindt er een jaarlijkse toetsing plaats om na te gaan of het waterschap in control is op het gebied van informatieveiligheid via peer reviews, audits of self-assessment?		Afwezig, alleen globaal gepland
Wat zijn de resultaten van deze toetsing?		Afwezig, nog niet uitgevoerd
Wordt de cyclus jaarlijks bijgesteld op basis van lessons learned?		Afwezig, nog niet uitgevoerd

Uitleg kleuren:
Groen = opzet en bestaan vastgesteld
Oranje = opzet en bestaan deels vastgesteld
Rood = opzet en bestaan afwezig

Bevindingen
De antwoorden zijn per deelvraag genoteerd.

2.4.1 *Functioneert de cyclus van informatieveiligheid binnen het waterschap?*

Vanaf 1 januari 2017 bestaat de in het document “Governance Informatiebeveiliging (procesmodel security board)” gedefinieerde cyclus van informatiebeveiliging binnen Rijnland waarmee jaarlijks een informatiebeveiligingsplan wordt gedefinieerd, uitgevoerd, gemonitord en geëvalueerd. Voor 2017 is dit plan pas zeer recent (juni 2017) vastgesteld. Het is volgens de adviseur informatievoorziening de bedoeling dat dit voor 2018 eind 2017 of uiterlijk begin 2018 gebeurt. Wij hebben hierdoor de complete functionering van de cyclus niet kunnen vaststellen. Wel hebben wij, door middel van verslagen van de security board, vastgesteld dat tijdens het project implementatie BIWA de planning en control hebben gefunctioneerd.

2.4.2 *Vindt er een jaarlijkse toetsing plaats om na te gaan of het waterschap in control is op het gebied van informatieveiligheid via peer reviews, audits of self-assessment?*

Nee, jaarlijkse toetsing moet conform de beschrijving van de cyclus van informatieveiligheid enerzijds plaatsvinden door een externe audit (door het Waterschapshuis) en anderzijds door een interne audit, uit te voeren door de CISO. Beiden hebben tot op heden nog niet plaatsgevonden. De externe audit staat op de (globale) planning voor najaar 2017, de interne audit wordt in ieder geval niet uitgevoerd vóór Q4 2017.

2.4.3 *Wat zijn de resultaten van deze toetsing?*

Van de toetsing zijn nog geen resultaten bekend omdat de cyclus in 2017 is ingevoerd en de toetsing nog niet is uitgevoerd.

2.4.4 *Wordt de cyclus jaarlijks bijgesteld op basis van lessons learned?*

De cyclus is nog niet bijgesteld op basis van lessons learned omdat de cyclus nog niet volledig is uitgevoerd.

2.5 Beveiligingsincidenten

Deelvragen	Status	Toelichting
Zijn er binnen het waterschap procedures opgesteld voor incidenten?		Afwezig
Welke risico's loopt Rijnland in geval van verstoring of cyberaanval, ook wanneer deze verstoring elders in de keten plaatsvindt?		Afwezig door ontbreken van inzicht in risico's, technisch onderzoek heeft echter diverse concrete risico's aangetoond
Hoeveel incidenten zijn er in de afgelopen periode (maand/half jaar) geweest?		0 gemelde incidenten maar inzicht niet gegarandeerd door ontbreken van procedure
Meldt Rijnland die incidenten bij de IBD?		0 gemelde incidenten maar inzicht niet gegarandeerd door ontbreken van procedure

Uitleg kleuren:
Groen = opzet en bestaan vastgesteld
Oranje = opzet en bestaan deels vastgesteld
Rood = opzet en bestaan afwezig

Bevindingen

De antwoorden zijn per deelvraag genoteerd.

2.5.1 *Zijn er binnen het waterschap procedures opgesteld voor incidenten?*

Nee, Rijnland heeft zoals hiervoor beschreven een incident management proces, maar dit is gericht op verstoringen van de operatie (conform ITIL) en bevat geen aspecten die relevant zijn voor informatiebeveiligingsincidenten zoals mogelijke melding naar Autoriteit Persoonsgegevens of aangifte bij de politie. Er is geen sprake van een formele vastlegging van de inrichting van de incidentregistratie. In het kader van de AVG is Rijnland bezig met het ontwikkelen van een procedure voor incidentregistratie.

2.5.2 *Welke risico's loopt Rijnland in geval van verstoring of cyberaanval, ook wanneer deze verstoring elders in de keten plaatsvindt?*

Als gevolg van een niet adequaat uitgevoerde risicoanalyse zijn deze risico's niet volledig in beeld. Deze risico's lopen uiteen van ransomware in de kantoorautomatisering tot het hacken van de procesautomatisering en het uitvallen van bedrijfsprocessen. Uit het technisch onderzoek blijkt dat zowel de kantoor- als de procesautomatisering onaanvaardbare kwetsbaarheden vertonen. Als

gevolg van deze kwetsbaarheden zijn in het technisch onderzoek onder andere de volgende punten aangetoond:

- Het was mogelijk om administrator rechten te verkrijgen op het kantoorautomatiseringsnetwerk van Rijnland. Hierdoor hadden de onderzoekers onder andere toegang tot: alle documenten van Rijnland, mogelijkheid om e-mail te lezen van alle werknemers waaronder de e-mail van de dijkgraaf, in te loggen op systemen namens alle werknemers, in te loggen op uiteenlopende servers en malafide software te installeren;
- Toegang tot systemen van de procesautomatisering voor bediening van AWZI's;
- Toegang tot het externe webportaal H@rm (salarisverwerking- en personeelsinformatiesysteem);
- Toegang tot externe webportaal Prosa (financieel administratief systeem);
- Ongecontroleerde fysieke toegang tot het gebouw van Rijnland.

2.5.3 *Hoeveel incidenten zijn er in de afgelopen periode (maand/half jaar) geweest?*

Het incidentenregister van Rijnland bevat geen enkel geregistreerd incident in het afgelopen half jaar. Door het ontbreken van een toereikende procedure kan de rekenkamercommissie geen uitspraak doen over de volledigheid van de incidentenregistratie.

2.5.4 *Meldt Rijnland die incidenten bij de IBD?*

Het incidentregister bevat geen actie richting toezichthouders. In de ambtelijke reactie is aangegeven dat er sinds 2013 – start van registratie van incidenten – geen aanleiding is geweest om actie te nemen richting toezichthouders.
In het kader van de AVG is Rijnland bezig met het ontwikkelen van een procedure voor incidentregistratie inclusief melding richting Autoriteit Persoonsgegevens, NCSC en / of politie.