BESTUURLIJKE NOTA INFORMATIEVEILIGHEID EN PRIVACYBESCHERMING (RC17.005)

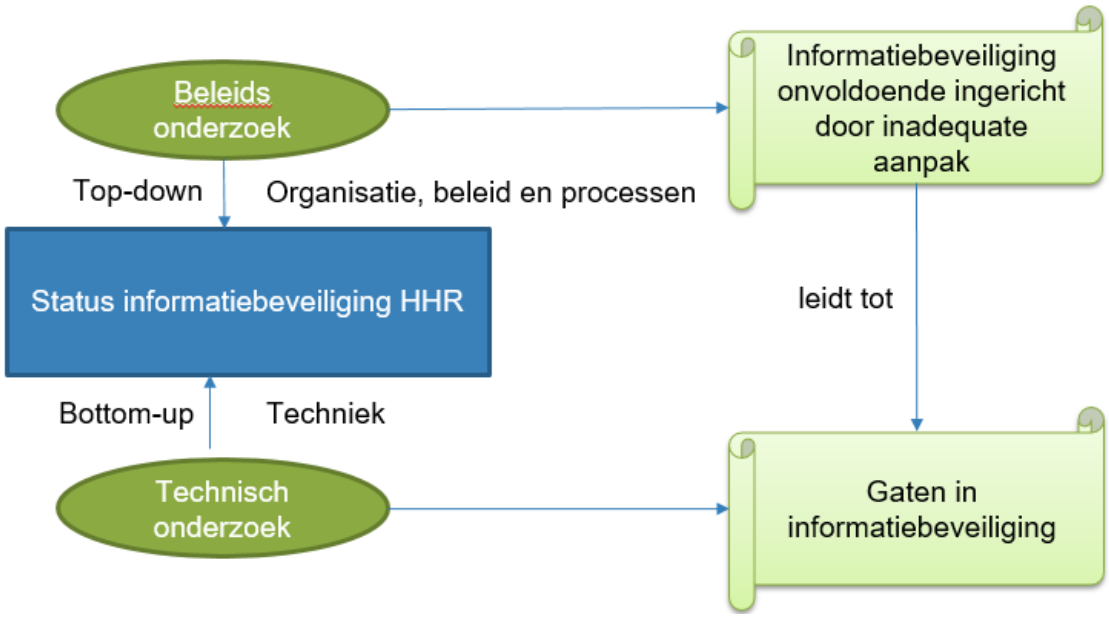
Inleiding
De rekenkamercommissie (RKC) van het Hoogheemraadschap van Rijnland heeft als taak en doel om de VV te ondersteunen bij de kaderstellende en controlerende rol van dit algemeen bestuur. Voor de VV is het belangrijk zicht te hebben op hoe Rijnland omgaat met informatieveiligheid en met de risico's die zij loopt, zowel technisch als bestuurlijk. Om de VV hierbij te ondersteunen heeft de RKC besloten, mede naar aanleiding van geuite wensen door het fractievoorzittersoverleg, een onderzoek in te stellen naar beleid en uitvoeringspraktijk van Rijnland op het gebied van informatieveiligheid en privacy. In het onderzoek stond de volgende vraag centraal:

> Is Rijnland 'in control' als het om informatieveiligheid en privacybescherming gaat?

De beantwoording van deze centrale onderzoeksvraag valt uiteen in de vijf onderzoeksvragen, die zijn beantwoord in de nota van bevindingen. In de nota van bevindingen is de aanpak van het onderzoek beschreven en zijn de gevonden feiten op de onderzoeksvragen gerapporteerd. De nota van bevindingen is als bijlage bij de voorliggende bestuurlijke nota gevoegd. In de bestuurlijke nota rapporteert de RKC de conclusies en aanbevelingen aan de VV

Aanpak: technisch en beleidsonderzoek in samenhang onderzocht
De rekenkamer heeft er bewust voor gekozen voor dit gevoelige onderzoek de samenwerking te zoeken met de ambtelijke organisatie en is verheugd over de zeer constructieve opstelling van de ambtelijke organisatie.

Het onderzoek is door de rekenkamercommissie op twee manieren uitgevoerd: een beleidsonderzoek (top-down) en een technisch onderzoek (bottom-up). Zowel het beleidsonderzoek als het technisch onderzoek hebben naar de informatiebeveiliging van Rijnland gekeken. Vanuit organisatie, beleid en processen blijkt dat het doel waartoe Rijnland is opgericht wordt ondersteund door bedrijfsprocessen, die weer afhankelijk zijn van informatiesystemen.
Deze informatiesystemen kennen een beveiligingscomponent. In het beleidsonderzoek is onderzocht of de informatiebeveiliging goed is georganiseerd. Daarbij wordt geconcludeerd dat binnen Rijnland deze informatiebeveiliging onvoldoende is ingericht. In het technisch onderzoek is de daadwerkelijke informatieveiligheid op de proef gesteld, waarbij een grote hoeveelheid tekortkomingen in de informatiebeveiliging is vastgesteld. Zie hieronder een schematische weergave van deze samenhang.



Beantwoording centrale onderzoekvraag
De hoofdconclusie van het onderzoek is, dat het hoogheemraadschap van Rijnland vooral op technisch vlak, maar ook op beleidsmatig vlak, niet 'in control' is, als het gaat om informatieveiligheid en privacybescherming. Hierdoor is Rijnland kwetsbaar.
Op basis van het onderzoek kan geconcludeerd worden dat het stelsel van interne controle samenhangend met informatiebeveiliging en privacybescherming onvoldoende werkt. Er is aandacht voor beleid en organisatie, maar de implementatie in procedures en technische maatregelen is onvoldoende. Deze 'onvoldoende' is gebaseerd op de slechts gedeeltelijk geïmplementeerde BIWA (zie hierna) en het ontbreken van een totaalinzicht in de risico's die Rijnland loopt op het gebied van informatiebeveiliging. De BIWA is landelijk opgesteld als een instrument in het kader van 'verplichtende zelfregulering' door onder meer de waterschappen.

Conclusie technisch onderzoek
Het technisch onderzoek heeft aangetoond dat feitelijk alle kernprocessen van Rijnland toegankelijk en manipuleerbaar waren voor een – door de rekenkamercommissie - ingeschakelde ethische hacker en dat deze toegang heeft verkregen tot privacygevoelige informatie.

Conclusie beleidsmatig onderzoek
Het beleidsmatig onderzoek heeft aangetoond dat:

- De Baseline Informatiebeveiliging Waterschappen (BIWA) gedeeltelijk is geïmplementeerd;
- Dat een integraal inzicht ontbreekt in de risico's die Rijnland loopt op het gebied van informatiebeveiliging;
- Dat hierdoor een integraal inzicht in de te treffen maatregelen ontbreekt.

De BIWA biedt een standaard set van maatregelen die – op lokaal niveau - leiden tot een basisbeveiligingsniveau. De BIWA beschrijft dat per te beveiligen object moet worden geanalyseerd of de BIWA afdoende is en vormt als zodanig slechts een deelverzameling van de totale te treffen maatregelen. Het is aan de individuele waterschappen, zoals Rijnland, om waar nodig *aanvullende* maatregelen te nemen die tezamen met de maatregelen uit het BIWA (op lokaal niveau) moeten leiden tot een adequaat beveiligingsniveau.
De tot nu toe door Rijnland uitgevoerde werkzaamheden zijn gebaseerd op een incomplete risicoanalyse, waardoor de volledigheid van het inzicht in de risico's niet gegarandeerd is. Rijnland heeft als uitgangspunt de maatregelen van de BIWA genomen en heeft daar risico's bij benoemd en geclassificeerd. De BIWA is een te eng vertrekpunt, waardoor niet alle risico's worden afgedekt.

In het rekenkamercommissie onderzoek is een analyse gemaakt aan de hand van vijf invalshoeken waarbij deelvragen zijn geformuleerd. In de nota van bevindingen staan de antwoorden op deze deelvragen gedetailleerd weergegeven, voorzien van een kleur waardoor de lezer eenvoudig toegang heeft tot het genuanceerde beeld van de uitkomsten van het onderzoek van de rekenkamercommissie.

De onderstaande tabel vat de antwoorden op de deelvragen (in de nota van bevindingen) samen.

Deelvraag	Kernbevinding, oordeel RKC
Taskforce BID/BIWA Hoe heeft het college uitvoering gegeven aan de adviezen van de Taskforce BID, zoals die specifiek voor waterschappen gegeven zijn?	Rijnland heeft in 2013 het informatie-beveiligingsbeleid vastgesteld en dit in 2016 aangepast op basis van het BIWA (advies van Taskforce BID). Vaststelling beleid door directieteam. De uitvoering is gaande.
Beleid en organisatie Hoe is het informatiebeveiligingsbeleid vormgegeven binnen het waterschap? Wie zijn er als verantwoordelijken aangesteld en is er aandacht voor bewustwording?	Rijnland heeft beleid vastgesteld en verantwoordelijkheden zijn belegd, maar niet alle rollen zijn voldoende bemenst. Er is aandacht voor bewustwording.
Risicoanalyse 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?	Rijnland is uitgegaan van de 133 maatregelen van de BIWA en niet van een risicoanalyse. Door gebruik van een incomplete risicoanalyse is er geen duidelijke afweging gemaakt bij de acceptatie van risico's. Het technisch onderzoek heeft aangetoond dat op dit moment de informatiebeveiliging en privacybescherming onvoldoende is.
Cyclus van informatiebeveiliging 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?	Rijnland heeft de cyclus voor informatie-beveiliging in 2017 opgezet, maar deze is nog niet volledig uitgevoerd Er worden (wettelijk verplichte) toetsingen uitgevoerd (DIGID, EDP), maar een audit naar informatieveiligheid is nog niet uitgevoerd.
Beveiligingsincidenten 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?	Rijnland heeft voor informatiebeveiligings-incidenten nog geen formele procedure ingericht. Er is wel een incidentenregister. Het technisch onderzoek heeft aangetoond dat Rijnland onaanvaardbare risico's loopt op het gebied van informatiebeveiliging en privacybescherming.

De beantwoording van de deelvragen leert, dat Rijnland beleid heeft opgesteld en er enig inzicht bestaat in de risico's, maar dat de feitelijke werking nog in ontwikkeling is. Ondertussen vertoont de informatiebeveiliging en privacybescherming onaanvaardbare gaten. Dit geeft de rekenkamercommissie aanleiding tot onderstaande aanbevelingen.

Aanbevelingen

Hieronder doet de rekenkamercommissie aan de VV vijf aanbevelingen, die onderlinge samenhang vertonen en opbouwen tot het ‘in control’ komen van het hoogheemraadschap van Rijnland op het gebied van informatieveiligheid en privacybescherming.

Aanbeveling 1 Dicht de gaten
De rekenkamercommissie beveelt de VV aan om het college, en daarmee de organisatie, opdracht te geven om de geconstateerde gaten in de informatiebeveiliging en privacybescherming zo snel mogelijk te dichten en de VV in 2017 (en 2018) per kwartaal te informeren over de mate waarin de gaten zijn gedicht.

Aanbeveling 2 Implementeer BIWA met voortvarendheid
De rekenkamercommissie beveelt de VV aan het college opdracht te geven de BIWA met voortvarendheid volledig te implementeren, omdat een deel van de maatregelen nog in de fase van planvorming staan.

Aanbeveling 3 Voer object-gerichte risicoanalyse uit
De rekenkamercommissie beveelt de VV aan het college opdracht te geven een objectgerichte risicoanalyse uit te voeren. Deze risicoanalyse zal aandachtspunten voor Rijnland opleveren, die ervoor zorgen dat Rijnland in control komt met betrekking tot informatieveiligheid en privacybescherming.

Aanbeveling 4 Implementeer verbetermaatregelen
De rekenkamercommissie beveelt de VV aan het college, en daarmee de organisatie, de opdracht te geven tot het implementeren van de (aanvullende) maatregelen, die voortvloeien uit de object-gerichte risicoanalyse , teneinde de informatiebeveiliging en privacybescherming in de organisatie te borgen en te verankeren.

Aanbeveling 5 Leg verantwoording af aan de VV
5a. De rekenkamercommissie beveelt de VV aan het college opdracht te geven aan de VV verantwoording af te leggen over de voortgang van de verbetermaatregelen (bijvoorbeeld in het door de rekenkamercommissie voorgestelde dashboard dat in ontwikkeling is) en aan de VV een ‘in control statement ‘ met betrekking tot de informatieveiligheid en privacybescherming af te geven.
5b. De rekenkamercommissie beveelt de VV aan het college de opdracht te geven om door het bestuur van de BSGR te laten aantonen dat de informatieveiligheid en privacybescherming bij de heffing en inning van waterschapsbelastingen (namens het hoogheemraadschap van Rijnland) in control is, zowel beleidsmatig als technisch.