



## Rapportage follow-up Rekenkamercommissie rapport informatiebeveiliging

De Rekenkamercommissie heeft de rapportage van de landelijke Taskforce Bestuur & Informatieveiligheid Dienstverlening (BID) van november 2014 als uitgangspunt genomen. Deze adviezen beschrijven de inrichting van de informatiebeveiliging op hoog niveau. Vervolgens heeft de rekenkamercommissie ingezoomd op een aantal specifieke onderwerpen. Een technische test door een ethisch hacker van de RKC heeft kwetsbaarheden aan het licht gebracht, aanvullend hierop organiseert Rijnland zelf her-testen door ethische hackers. In deze rapportage wordt op hetzelfde niveau als in de rapportage van de rekenkamercommissie de actuele stand van zaken weergegeven. In de toelichting onder 2.5 worden bijzonderheden aangegeven over de aanpak van de kwetsbaarheden, inclusief de leerpunten uit de her-testen.

### Adviezen BID

|  |   |
|--|---|
|  | 0 |
|  | 1 |
|  | 7 |

### Specifieke onderwerpen

|  |    |
|--|----|
|  | 1  |
|  | 2  |
|  | 11 |

### Herstel kwetsbaarheden



Status van de reparatie van de door de RKC aangetroffen kwetsbaarheden.

Datum rapportage: 29 mei 2018

Uitleg kleuren in deze rapportage:

Groen = opzet en bestaan vastgesteld

Oranje = opzet en bestaan deels vastgesteld

Rood = opzet en bestaan afwezig

Archimedesweg 1  
postbus 156  
2300 AD Leiden

KvK nr: 51137747

telefoon: (071) 30 63 063  
internet: [www.rijnland.net](http://www.rijnland.net)  
e-mail: [post@rijnland.net](mailto:post@rijnland.net)

BTW nr: NL813766928B01

Rijnland streeft naar een transparant relatiebeheer met duidelijke regels over belangenverstrengeling en het aannemen van giften.  
Meer weten? Wij verwijzen u graag naar onze Algemene Voorwaarden.



## 2.1 Opvolging adviezen Taskforce BID

| Deelvragen                                                                                                      | Status RKC | Status 2018Q1 | Status 2018Q2 | Toelichting                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------|------------|---------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Het opstellen en vaststellen van een beleidsplan informatieveiligheid met doelen, maatregelen en budget         |            |               |               | Het informatiebeveiligingsbeleid is actueel. In april 2018 is het Informatiebeveiligingsplan 2018-2019 bekrachtigd in de I-raad (werkversie) en deze wordt in het Dt geagendeerd ter vaststelling.                                                                                                                                                                                                                                                                                                                        |
| Het in de begroting opnemen van het benodigde budget om informatieveiligheid adequaat in te kunnen richten      |            |               |               | Het DT heeft in januari 2018 besloten een specifiek budget voor informatiebeveiliging te alloceren. Is geregeld voor 2018. Dit is inmiddels in de MJP-voorbereiding opgenomen tbv opname in de begroting 2019 e.v.                                                                                                                                                                                                                                                                                                        |
| De implementatie van de Baseline Informatiebeveiliging Waterschappen (BIWA)                                     |            |               |               | De landelijke audit van het Waterschapshuis heeft laten zien dat van de 44 BIWA doelstellingen Rijnland op 25 grotendeels voldoet en op 19 deels voldoet. Op geen enkele doelstelling is het oordeel "voldoet beperkt". In het Informatiebeveiligingsplan zijn veel actie s opgenomen die de mate van voldoen aan de BIWA zullen vergroten. Rijnland bevindt zich met de uitslag met Schieland en de Krimpenerwaard inmiddels bij de twee hoogst scorende waterschappen. Gestuurd wordt om eind 2019 volledig te voldoen. |
| Het inrichten van een PDCA-cyclus informatieveiligheid als onderdeel van de reguliere Planning & Control-cyclus |            |               |               | De PDCA-cyclus voor informatiebeveiliging functioneert en sluit aan op de reguliere P&C-cyclus.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Het meten van informatieveiligheid aan de hand van indicatoren                                                  |            |               |               | De i-Raad monitort de informatieveiligheid per kwartaal aan de hand van 42 KPI's. Indien nodig schakelt de i-raad op naar de directie.                                                                                                                                                                                                                                                                                                                                                                                    |
| Het aanleveren van de meting naar de koepel (UvW) ten behoeve van een beeld over de overheidslaag               |            |               |               | Naast de initiële meting is eind 2017 een landelijke BIWA-audit georganiseerd door het Waterschapshuis. Rijnland heeft hier alle gegevens voor aangeleverd.                                                                                                                                                                                                                                                                                                                                                               |
| Het treffen van voorbereidingen voor een audit op informatieveiligheid                                          |            |               |               | Ten behoeve van de landelijke BIWA-audit zijn vele bewijsstukken verzameld en aangeleverd. In 2018 wordt een interne audit gehouden. Hieraan gerelateerd worden ook technische testen uitgevoerd, zie hiervoor ook paragraaf 2.4.                                                                                                                                                                                                                                                                                         |
| Het inrichten van incidentregistratie en incidentrapportages                                                    |            |               |               | De incidentregistratie van informatiebeveiligingsincidenten is uitgewerkt, ingericht en geïntegreerd in het reguliere systeem voor incidentregistratie. In                                                                                                                                                                                                                                                                                                                                                                |



| Deelvragen | Status RKC | Status 2018Q1 | Status 2018Q2 | Toelichting                              |
|------------|------------|---------------|---------------|------------------------------------------|
|            |            |               |               | de i-Raad wordt de rapportage besproken. |

## 2.2 Bevindingen RKC: Beleid en organisatie

| Deelvragen                                                                 | Status RKC | Status 2018Q1 | Status 2018Q2 | Toelichting                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------|------------|---------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hoe is het informatiebeveiligingsbeleid vormgegeven binnen het waterschap? |            |               |               | Het informatiebeveiligingsbeleid is actueel, in april 2018 is een nieuw informatiebeveiligingsplan bekrachtigd ter vaststelling in het Dt.                                                                                                                                                                                                      |
| Wie zijn er als verantwoordelijken aangesteld?                             |            |               |               | De verschillende rollen op het gebied van informatiebeveiliging zijn ingevuld. Januari 2018 is een nieuwe security officer (CISO) benoemd. Er is ter versterking van de informatiebeveiligingsorganisatie een nieuwe rol gedefinieerd: Operational Security Officer, die is aangesteld per 1 mei 2018                                           |
| Is er aandacht voor bewustwording?                                         |            |               |               | Er is op verschillende fronten aandacht voor bewustwording. Dit onderwerp is nooit klaar, medewerkers en bestuursleden moeten meegroeien in hun weerbaarheid met de toenemende dreigingen vanuit de wereld om ons heen. Inmiddels is er een lopende actie om in het voorjaar 2018 de 10 gouden regels structureel onder de aandacht te brengen. |



### 2.3 Bevindingen RKC: Risicoanalyse

| Deelvragen                                                                                                              | Stat<br>us<br>RK<br>C | Status<br>2018Q1 | Status<br>2018Q2 | Toelichting                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------|-----------------------|------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Welke risico's accepteert het college en welke niet?                                                                    |                       |                  |                  | De objectgerichte risico-analyse is gestart met de eerste drie objecten (Ultimo/Airwatch/IBabs). Het uitvoeren van een objectgerichte risico-analyse is veel werk door de grote hoeveelheid objecten en er wordt gezocht naar een efficiënte methode. Bespreking in het college is voorzien in 2019.                                                                                                                     |
| Welke politiek-bestuurlijke en maatschappelijke gevolgen kan dit hebben in geval van een incident?                      |                       |                  |                  | Deze vraag is nog niet eenduidig te beantwoorden, dit kan op basis van de uitkomsten van de risico-analyse.                                                                                                                                                                                                                                                                                                              |
| Is de privacy van de burgers, bedrijven en overige belanghebbenden gegarandeerd? Ook in relatie tot verbonden partijen? |                       |                  |                  | Er is een FG aangesteld. Het privacybeleid is vastgesteld.. Geinventariseerd is in welke systemen persoonsgegevens worden verwerkt. De nog te nemen maatregelen zijn bekend. De Implementatie van een aantal maatregelen loopt nog door na 25 mei, maar Rijnland voldoet tijdig aan de formele eisen van de AVG. De BSGR heeft een eigen verantwoordelijkheid en heeft eveneens FG aangesteld en een beleid vastgesteld. |



#### 2.4 Bevindingen RKC: Cyclus van informatieveiligheid

| Deelvragen                                                                                                                                                                | Status RKC | Status 2018Q1 | Status 2018Q2 | Toelichting                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Functioneert de cyclus van informatieveiligheid binnen het waterschap?                                                                                                    |            |               |               | De PDCA-cyclus van informatiebeveiliging functioneert. De verbeterpunten uit 2017 zijn meegenomen in het informatiebeveiligingsplan 2018.                                                                                                                                                                                                     |
| 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? |            |               |               | Rijnland heeft meegedaan in de landelijke audit die het Waterschapshuis heeft georganiseerd. In 2018 is een interne audit voorzien. Daarnaast laat Rijnland de infrastructuur jaarlijks testen door een ethische hacker. In dat kader is ook een hertest uitgevoerd door dezelfde ethische hacker die de rekenkamercommissie heeft ingehuurd. |
| Wat zijn de resultaten van deze toetsing?                                                                                                                                 |            |               |               | De landelijke audit van het Waterschapshuis heeft laten zien dat van de 44 BIWA doelstellingen Rijnland op 25 grotendeels voldoet en op 19 deels voldoet. Op geen enkele doelstelling is het oordeel "voldoet beperkt".                                                                                                                       |
| Wordt de cyclus jaarlijks bijgesteld op basis van lessons learned?                                                                                                        |            |               |               | De adviezen uit de audit 2017 zijn meegenomen in het informatiebeveiligingsplan 2018.                                                                                                                                                                                                                                                         |



## 2.5 Bevindingen RKC: Beveiligingsincidenten

| Deelvragen                                                                                                                        | Status RKC | Status 2018Q1 | Status 2018Q2 | Toelichting                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------|------------|---------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Zijn er binnen het waterschap procedures opgesteld voor incidenten?                                                               |            |               |               | De incidentregistratie van informatiebeveiligingsincidenten is uitgewerkt, ingericht en geïntegreerd in het reguliere systeem voor incidentregistratie. In de i-raad wordt de rapportage besproken. Indien nodig wordt opgeschaald naar de directie.                                                                                                                                                                                                                                                                           |
| Welke risico's loopt Rijnland in geval van verstoring of cyberaanval, ook wanneer deze verstoring elders in de keten plaatsvindt? |            |               |               | Van de kwetsbaarheden die de rekenkamercommissie heeft gesignaleerd is 97% volledig opgelost (eerste kwartaal was dat 89%). Wat resteert is de Unix server, die in mei door een Windows server wordt vervangen en het updaten van ene restant thin clients. 100% van de kritische bevindingen is opgelost. De organisatie heeft een hertest laten uitvoeren en zal verder jaarlijks een technische test laten doen door een ethische hacker. Bevindingen die voortkomen uit de hertest zijn geprioriteerd en worden aangepakt. |
| Hoeveel incidenten zijn er in de afgelopen periode (maand/half jaar) geweest?                                                     |            |               |               | De nieuwe incidentregistratie is december 2017 gestart. In het eerste kwartaal 2018 zijn tot nu toe 10 incidenten geregistreerd. De incidenten worden via een oplosgroep afgehandeld en er worden maatregelen ingezet om dergelijke incidenten in de toekomst te voorkomen. De interne bewustwordingsactie heeft tot meer meldingen geleid en dat is juist goed.                                                                                                                                                               |
| Meldt Rijnland die incidenten bij de autoriteiten?                                                                                |            |               |               | In 2018 is één incident gemeld bij de Autoriteit persoonsgegevens of andere autoriteiten. Tevens is Rijnland aangesloten op het CERT watermanagement, het samenwerkingsverband van de waterschappen met Rijkswaterstaat voor snelle respons op dreigende incidenten (buiten het domein persoonsgegevens).                                                                                                                                                                                                                      |