REKENKAMERCOMMISSIE
RIJNLAND

RAPPORT

Grip op informatieveiligheid

Onderzoek naar de beheersing van de veiligheid van informatie bij Rijnland

van de rekenkamercommissie van
het hoogheemraadschap van Rijnland

Rapport onderzoek informatieveiligheid

Leiden, 31 augustus 2023

Corsanummer: 23.091345

Dit onderzoek is uitgevoerd door Berenschot in opdracht van de rekenkamercommissie van het hoogheemraadschap van Rijnland.

REKENKAMERCOMMISSIE RIJNLAND

Berenschot

Voorwoord

Informatieveiligheid is een thema dat volop in de schijnwerpers staat. Hoe vaak horen we niet in het nieuws of lezen we in de krant dat een overheid, bedrijf of instelling getroffen is door een hack of een phishing mail? Door de toenemende digitalisering is het zorgvuldig omgaan met informatie, systemen en gegevens van steeds groter belang.

De rekenkamercommissie van het hoogheemraadschap van Rijnland (RKC) wilde daarom graag onderzocht hebben of de informatieveiligheid bij Rijnland voldoende is geborgd. In het bijzonder is gekeken naar de wijze waarop de verenigde vergadering, het college van dijkgraaf en hoogheemraden en de ambtelijke organisatie invulling geven aan informatieveiligheid en hoe het samenspel tussen deze drie lagen plaatsvindt.

De RKC bedankt onderzoeksbureau Berenschot voor haar werkzaamheden. Ook dank aan de betrokken ambtenaren en portefeuillehouder voor de prettige en constructieve samenwerking. In het bijzonder kijkt de rekenkamercommissie terug op een waardevolle en goede samenwerking met de CISO.

We hopen dat de verenigde vergadering met dit onderzoek in handen een goede dialoog kan voeren met het college van dijkgraaf en hoogheemraden. De RKC wenst de verenigde vergadering veel succes met het stellen van kaders en het controleren daarvan met betrekking tot de informatiebeveiliging. De RKC wenst ook het college en de ambtelijke organisatie veel succes met de ontwikkelingen op dit belangrijke beleidsterrein.

Leeswijzer

Het rapport is opgebouwd uit twee delen. Het eerste deel is de bestuurlijke nota en is een op zichzelf leesbaar rapport. Hierin wordt een managementsamenvatting gegeven, gevolgd door de conclusies en aanbevelingen. De bestuurlijke reactie van het college is integraal opgenomen. Het nawoord van de rekenkamercommissie sluit de bestuurlijke nota af.

Deel twee is de nota van bevindingen. Hierin is het integrale onderzoek opgenomen met daarin de beantwoording van de onderzoeksvragen en de onderbouwing van de conclusies en aanbevelingen.

BESTUURLIJKE NOTA

1. Management samenvatting

Door de toenemende digitalisering is het zorgvuldig omgaan met informatie, systemen en gegevens van burgers voor waterschappen van groot belang. Een betrouwbare, beschikbare en correcte informatiehuishouding en veilige systemen zijn essentieel voor de dienstverlening. Hiervoor is het noodzakelijk dat de ambtelijke organisatie en het bestuur van een waterschap een goed samenspel met elkaar hebben, zodat strategische, tactische en operationele zaken in samenhang plaatsvinden.

De rekenkamercommissie heeft om die reden een onderzoek laten uitvoeren naar de mate waarin het bestuur van het Hoogheemraadschap van Rijnland in control is als het gaat om informatieveiligheid. Hierbij is gekeken naar de organisatorische inrichting, rapportages, risicomanagement, en de plan-do-check-act cyclus. Meer in het bijzonder is gekeken naar de wijze waarop verenigde vergadering als algemeen bestuur, het college van dijkgraaf en hoogheemraden als dagelijks bestuur en de ambtelijke organisatie invulling geven aan deze onderwerpen en hoe het samenspel tussen deze drie lagen plaatsvindt. In het kader van het onderzoek is gekeken naar de relevante documentatie, zijn de openbare stukken van de verenigde vergadering bekeken en zijn interviews afgenomen binnen de drie verschillende lagen.

Uit het onderzoek blijkt dat het hoogheemraadschap van Rijnland een organisatie is die in beweging is op het gebied van digitale transformatie. Hierdoor is weliswaar nog niet op alle onderwerpen het ideale samenspel gevormd, maar is wel zichtbaar dat de organisatie op weg is naar een stevige organisatie op het gebied van informatieveiligheid. De geconstateerde verbeterpunten zijn veelal al door de organisatie zelf gesignaleerd, en in vele gevallen is de weg naar verbetering reeds ingeslagen.

Dit betekent dat de hoofdvraag *"Is het bestuur van het hoogheemraadschap van Rijnland in control ten aanzien van informatieveiligheid?"* als volgt beantwoord wordt: **het bestuur is de afgelopen jaren meer in control gekomen en zal door een sterkere inbedding van risicomanagement in rapportages en besluitvorming en een nadrukkelijkere invulling van de controlerende taak de komende jaren beter in staat komen om in control te zijn.** Belangrijkste aanbevelingen hierbij die volgen uit het onderzoek zijn:

1) investeer in het vergroten van de inhoudelijke kennis van de leden van de verenigde vergadering, zodat het juiste gesprek kan plaatsvinden tussen de drie lagen;
2) zet door op de ingezette weg voor het verbeteren van de rapportages aan D&H en VV. Denk met name aan strategisch/tactisch gerichte rapportages die bijvoorbeeld inzicht geven in de algehele staat van informatiebeveiliging, in de manier waarop dreigingen, risico's en maatregelen zich tot elkaar verhouden en in de effectiviteit van genomen maatregelen. Dergelijke rapportages vormen een belangrijke schakel voor het noodzakelijke samenspel tussen de drie lagen;
3) houdt vast aan de ingezette koers, want deze koers zal zorgen voor de gewenste versterking van de informatieveiligheidsorganisatie.

2. Conclusies

Hoogheemraadschap van Rijnland is als organisatie sterk in beweging om te transformeren naar een datagedreven organisatie. Hiermee wordt uitvoering gegeven aan de ambities die de VV in besluitnota's heeft vastgesteld. In de uitvoeringsprogramma's zien we dat HHR stevige ambities heeft ten aanzien van zijn ICT en informatievoorziening. De onderwerpen informatiebeveiliging en privacy zijn expliciet onderdeel van deze geformuleerde ambities en worden randvoorwaardelijk geacht voor een succesvolle transformatie. Voor de ICT-voorziening werkt HHR nauw samen met hoogheemraadschap van Schieland en Krimpenerwaard. Beide organisaties delen de ICT-infrastructuur en hebben ervoor gekozen om ook op het gebied van beleid, governance en functies volledig samen te werken. De belangrijkste drijfveer voor deze samenwerking is gelegen in kosteneffectiviteit en -efficiëntie.

Deze ambities hebben de afgelopen jaren dan ook geleid tot een aantal grote stappen op het gebied van informatiebeveiliging. Zo heeft men de organisatie ingericht naar het Three Lines of Defense model en de posities van Chief Information Security Officer en Functionaris Gegevensbescherming verder verstevigd. Het (vernieuwde) Strategisch IB beleid definieert heldere uitgangspunten en beschrijft op heldere wijze hoe verschillende functies zich tot elkaar verhouden binnen de ambtelijke organisatie. Tegelijkertijd merken we op dat op basis van de aangeleverde documentatie het beeld ontstaat dat de ambtelijke organisatie binnen HHR nog druk bezig is met het implementeren van diverse beheersmaatregelen. Voorbeelden hiervan zijn de rapportages die vooral op operationeel niveau een beeld geven van de risico's en dreigingen. Dit beeld wordt bevestigd in de interviews en men geeft aan druk bezig te zijn om de informatievoorziening op tactisch/strategisch niveau verder te verbeteren. Dit betekent wel dat momenteel rapportage, besluitvorming, en controle meer ad hoc en regelmatig op informele wijze plaatsvindt. Hierdoor is het niet altijd duidelijk hoe ambities zich verhouden tot concrete risico's en op welke wijze de daarop genomen beheersmaatregelen bijdragen aan het mitigeren van deze risico's. Doordat de organisatie nog volop in ontwikkeling is, is het lastig om heldere inzichten op strategisch niveau te koppelen aan investeringen in informatiebeveiliging en het mitigeren van risico's. De organisatie is zich hier duidelijk van bewust en geeft expliciet aan hier mee bezig te zijn.

Bovenstaande heeft naar ons oordeel momenteel dan ook de nodige impact op de wijze waarop de verschillende gremia (VV, D&H, en ambtelijke organisatie) zich tot elkaar verhouden.

De ambtelijke organisatie bevindt zich momenteel te midden van de digitale transformatie en is daarmee volop in beweging. Op het gebied van informatiebeveiliging zien we dat het een aantal grote stappen zet om de volwassenheid op het gebied van informatiebeveiliging te verhogen. Het vernieuwen van het informatiebeveiligingsbeleid, waarbij de governance opnieuw is ingericht en de focus ligt op risico-gebaseerd sturen en het continu monitoren en evalueren van beheersmaatregelen bevestigen dit. Wel valt ons op dat de periodieke rapportages die we hebben ontvangen vooral gericht zijn op operationeel niveau. De rapportages die met ons zijn gedeeld over het aantal incidenten en informatiebeveiligingsrisico's geven vooral inzicht in de staat in concrete gevallen, maar geven relatief weinig inzicht in de algehele staat van informatiebeveiliging. Bestuurlijke besluitvorming en conclusies lijken vooralsnog dan ook vooral plaats te vinden op basis van de (informele) toelichting aan en overleg met de portefeuillehouder.. De VV en D&H zouden meer baat hebben bij inzichten in de effectiviteit van genomen maatregelen.
D&H als geheel lijkt op dit moment een beperkte rol te vervullen op het gebied van informatiebeveiliging. Het vertrouwen van D&H en VV in de ambtelijke organisatie is groot. Dit

vertrouwen is mooi om te zien, maar een bepaalde mate van controle is ook nodig op het gebied van informatiebeveiliging. De gevolgen van (cyber)incidenten kunnen een enorme impact hebben op de organisatie en daarom is het van belang om, gegeven de toenemende dreigingen op dit gebied, elkaar scherp te houden. De rol van D&H is zeer strategisch van aard. Een verschuiving naar strategisch/tactisch kan meer verbinding leggen tussen D&H en de ambtelijke organisatie. Hiervoor is onder meer nodig dat de ambtelijke organisatie op het juiste niveau D&H voorziet van informatie/rapportage op het gebied van informatiebeveiliging.

De VV geeft aan ten aanzien van haar kaderstellende en controlerende rol vooral op strategisch niveau invloed uit te willen oefenen op de wijze waarop informatiebeveiliging binnen HHR is ingericht. Uit het interview met enkele leden van de VV kwam naar voren dat men informatiebeveiliging vooral ziet als iets wat randvoorwaardelijk is aan de informatievoorziening en op dit onderdeel vooral ook te vertrouwen op D&H en de ambtelijke organisatie omdat de inhoudelijke kennis van informatiebeveiliging beperkt is binnen de VV. Ondanks het uitgesproken vertrouwen in de ambtelijke organisatie valt op dat dit toch leidt tot een ongemakkelijk gevoel bij een deel van de leden. Informatie rondom cybersecurity is vaak abstract (bijvoorbeeld hogere dreiging door de oorlog in Oekraïne) en daardoor lastig te vertalen naar concrete kaders of te monitoren. Dit leidt er onder meer toe dat het lastig is voor de VV om te bepalen welke maatregelen noodzakelijk zijn en welk risicoprofiel past bij de organisatie. De VV zal beter in staat zijn om haar kaderstellende en controlerende taken uit te voeren, wanneer periodieke rapportages over informatiebeveiliging op gestructureerde wijze laten zien hoe dreigingen, risico's en maatregelen zich tot elkaar verhouden. Concreet betekent dit dat informatie over informatiebeveiliging naar de VV inzichten dient te bieden in de wijze waarop het de ambities en visie beïnvloedt.

Afsluitend zien we dat veel van de geconstateerde zaken nadrukkelijk reeds onder de aandacht zijn van de ambtelijke organisatie. De duidelijke visie die men heeft over de doorontwikkeling van informatiebeveiliging binnen de organisatie geeft ons het vertrouwen dat de komende jaren de benodigde stappen gezet worden om ook het bestuur van de organisatie nadrukkelijker een rol te laten spelen op het gebied van risicomanagement en de PDCA-cyclus, onder andere door verbeterde rapportages en meer bewustwording.

Dit betekent dat wij de hoofdvraag *"Is het bestuur van het hoogheemraadschap van Rijnland in control ten aanzien van informatieveiligheid?"* als volgt beantwoorden: het bestuur is de afgelopen jaren meer in control gekomen, maar zal door een sterkere inbedding van risicomanagement in rapportages en besluitvorming en een nadrukkelijkere invulling van de controlerende taak de komende jaren beter in staat komen om in control te zijn.

3. Aanbevelingen

Op basis van de conclusies hebben wij enkele aanbevelingen voor HHR op het gebied van informatiebeveiliging.

Allereerst adviseren wij te investeren in het vergroten van de inhoudelijke kennis van de VV op het gebied van informatiebeveiliging. Daarmee bedoelen we absoluut niet dat elk lid van de VV een inhoudelijke opleiding behoeft om de rol van de VV te kunnen uitvoeren. Echter, een beperkte investering om de basisprincipes van informatiebeveiliging te begrijpen en de VV enkele handvatten te geven over de wijze waarop het gesprek over dit onderwerp gevoerd kan worden, verdiept het gesprek in de VV en geeft de vergadering de mogelijkheid haar rol beter te spelen. Indirect zal dit – naar verwachting – de informatiebeveiliging binnen de ambtelijke organisatie versterken door een sterkere werking van de PDCA-cyclus en een betere inbedding van risicomanagement binnen besluitvorming. Binnen gemeentes heeft de VNG bijvoorbeeld voor gemeenteraadsleden een Checklist digitale veiligheid[1] uitgebracht. Een dergelijk hulpmiddel kan bijdragen aan het goede gesprek over informatiebeveiliging en geeft de VV-leden die minder kennis hebben van het onderwerp meer comfort om het gesprek aan te gaan over het onderwerp.

Ten tweede ondersteunen we de ingezette route om de rapportages te verbeteren. Wij bevelen aan om de rapportages voor de VV meer te richten op de staat van de informatiebeveiliging. Met andere woorden, geef niet alleen inzicht in de verbeteracties die lopen, maar informeer de VV ook over de volledige stand van zaken van de organisatie. Kijk hierbij naar bijvoorbeeld welke dreigingen momenteel groot dan wel groeiend zijn, welke (strategische) risico's de organisatie in beeld heeft en of er al dan niet maatregelen gekoppeld zijn aan de geconstateerde risico's. Daarbij versterkt meer informatie richting D&H over de stand van zaken op specifieke maatregelen en informatie over meer tactische risico's de informatiepositie van D&H. Met dergelijke verbeterde rapportages worden zowel de VV als D&H beter in staat gesteld om hun functie te vervullen.

Tot slot bevelen wij aan vooral de ingezette koers vast te houden. We zien een organisatie die goede stappen zet in de digitale transformatie. Op basis van wat we gezien hebben, verwachten wij dat de ingezette stappen ook bijdragen aan een steviger samenspel tussen de gremia dan nu reeds het geval is.

[1] https://vng.nl/sites/default/files/2023-02/Checklist_raadsleden_Digitale_Vaardigheden.pdf

4. Bestuurlijke reactie

Hoogheemraadschap van
Rijnland

uw kenmerk:
uw brief van:
ons kenmerk: 23.051858 /
bijlagen:
Inlichtingen: Marlou Veloo, Jasper de Vries
doorkiesnummer: +31713063224
onderwerp: Bestuurlijke reactie onderzoeksrapport Rekenkamercommissie

Rekenkamercommissie Rijnland
T.a.v. de heer Pieters
Postbus 156
2300AD LEIDEN

Leiden, **07-07-2023**

Geachte heer Pieters,

Het college van dijkgraaf en hoogheemraden dankt de Rekenkamercommissie voor het onderzoeksrapport naar de beheersing van de veiligheid van informatie bij Rijnland. Wij ondersteunen de inhoud ervan en kunnen ons vinden in de conclusies en aanbevelingen die door de rekenkamercommissie zijn beschreven.

Algemeen
Wij zijn content met de ontwikkeling van het bestuur waarin besluitvorming in steeds grotere mate op basis van risico inschatting wordt gedaan en wij daarmee steeds meer in control komen op dit onderwerp. Daarnaast zijn wij blij met uw bevinding dat ondanks de grote digitale veranderingen binnen onze organisatie de knelpunten door de ambtelijke organisatie worden geïdentificeerd en actief opgepakt.

Onderzoek
Met betrekking tot de uitvoering van het onderzoek wil het college enkele kanttekeningen plaatsen. Kijkend naar de vermelde geraadpleegde stukken in het rapport meent het college dat het aantal onderzochte bestuurlijke stukken in omvang zeer gering is. Het rapport spreekt weliswaar over een steekproef op de notulen op het onderwerp informatieveiligheid, toch bevreemd het college zich over het feit dat er geen systematischer onderzoek heeft plaatsgevonden op de bestuurlijke rapportages en notulen. Beiden zijn immers belangrijke elementen in het verantwoording afleggen van het dagelijks bestuur en de controlerende functie van het algemeen bestuur.

Daarnaast vragen wij uw aandacht voor de opzet van het interview dat is afgenomen met verschillende leden van de VV. Het college is van mening dat de aansluiting tussen enerzijds de vragen in het interview en anderzijds de te beantwoorden hoofdvraag onvoldoende is. Het college zou graag zien dat hier een kwaliteitsslag wordt gemaakt. Deze kanttekeningen zijn eerder in het proces al aan de RKC en de ingehuurde partij, Berenschot, overgebracht. Het college verzoekt de RKC om te reflecteren op het onderzoeksproces na het ontvangen van deze signalen.

Archimedesweg 1
Postadres:
Postbus 156
2300 AD Leiden

KvK nr:51137747

telefoon: (071) 30 63 063
telefax: (071) 51 23 916
internet: www.rijnland.net
e-mail: post@rijnland.net

BTW nr: NL813766928B01

23.051858

Hoogheemraadschap van
Rijnland

Bestuur
We erkennen dat de inhoudelijke kennis over informatieveiligheid niet bij iedere bestuurder toereikend is om de aangeleverde rapportages juist te kunnen interpreteren om zo te komen tot goede besluitvorming. Dit geldt voor zowel het dagelijks als het algemeen bestuur. Rapportages passend bij het niveau van besluitvorming zouden daar ook bij kunnen helpen. Dit geldt eveneens voor het verhogen van de (basis)kennis van bestuursleden. In nauwe samenwerking met de ambtelijke organisatie, maar ook met partners als de Unie van Waterschappen, Het Waterschapshuis, andere waterschappen en het Rijk willen we hier de komende jaren samen met het algemeen bestuur invulling aan geven. Het aanbieden van een kennissessie over informatiebeveiliging om elke algemeen bestuurder van (basis)kennis te voorzien kan hier een belangrijke start in vormen.

Concluderend
Het college dankt de Rekenkamercommissie voor haar rapport. Wij onderschrijven de conclusies en zijn voornemens de aanbevelingen uit uw rapport over te nemen. Het college vraagt aandacht voor de gebruikte onderzoeksmethode en zou graag zien dat hier een kwaliteitsslag op wordt geboekt.

Middels een VV-besluitnota zullen wij verschillende aanbevelingen aanbieden aan het algemeen bestuur. Hiermee willen wij de aanbevelingen op korte termijn te vertalen naar beleid.

Met vriendelijke groet,

dijkgraaf en hoogheemraden,

Elektronisch getekend door Mariël Middendorp
op 07-07-2023

Rogier van der Sande,
dijkgraaf

Elektronisch getekend door Rogier van der Sande
op 07-07-2023

Mariël Middendorp,
Secretaris /Algemeen Directeur

5. Nawoord

De rekenkamercommissie dankt het college voor de bestuurlijke reactie. De rekenkamercommissie waardeert het dat het college voornemens is de aanbevelingen uit het rapport over te nemen. Het college onderschrijft de conclusies, maar vraagt ook aandacht voor de gebruikte onderzoeksmethode en zou graag zien dat hier een kwaliteitsslag op wordt geboekt. Over de uitvoering van dit onderzoek heeft de rekenkamercommissie in een eerder stadium gesproken met het college en de onderzoekers.

Om een onderzoek goed uit te kunnen voeren is de rekenkamercommissie afhankelijk van aanlevering van documenten door de organisatie. Bij dit onderzoek heeft die aanlevering in etappes plaatsgevonden. In bijlage 1 verwijzen de onderzoekers naar de documentatie die zij bij aanvang van het onderzoek hebben ontvangen. Ze hebben daarnaast zelf nog onderzoek gedaan naar documenten die Rijnland de afgelopen jaren gepubliceerd heeft (op basis van diverse zoektermen). Ze hebben dus juist heel veel documenten bekeken, maar er is helaas weinig relevants gevonden over het onderwerp informatieveiligheid. De rekenkamercommissie betreurt het dat er onduidelijkheid over de onderzochte bestuurlijke stukken is ontstaan door het feit dat bijlage 1 niet compleet is en door de gekozen formulering 'steekproefsgewijs'.

De rekenkamercommissie heeft (de opzet van) het interview dat is afgenomen met verschillende leden van de VV geëvalueerd. Zij deelt de mening van het college dat hier een kwaliteitsslag moet worden gemaakt en heeft verschillende verbeterpunten geformuleerd.

De rekenkamercommissie gaat uiteraard graag met het college en de verenigde vergadering in gesprek over dit rapport, als ook over de onderzoeksmethoden van de rekenkamercommissie.
Tot slot bedankt de rekenkamercommissie alle betrokkenen voor hun bijdrage aan dit onderzoek.

NOTA VAN BEVINDINGEN

1. Aanleiding en onderzoeksopzet

1.1. Aanleiding

Door de toenemende digitalisering is het zorgvuldig omgaan met informatie, systemen en gegevens van burgers voor waterschappen van groot belang. Uitval van computers of systemen, het in ongerede raken van gegevensbestanden of het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de continuïteit van de bedrijfsvoering en het primaire proces. Een betrouwbare, beschikbare en correcte informatiehuishouding en veilige systemen zijn essentieel voor de dienstverlening. De afgelopen jaren is de aandacht voor informatieveiligheid[2] ontzettend gegroeid. Tegelijkertijd blijkt uit incidenten dat de basis voor informatiebeveiliging bij lang niet alle organisaties op voldoende niveau is. Inzicht hebben in de stand van zaken bij een organisatie is nodig om bij te kunnen sturen en te verbeteren en zo weerstand te bieden tegen dreigingen. De rekenkamercommissie (RKC) van het hoogheemraadschap van Rijnland (HHR) wilde daarom graag onderzocht hebben of de informatieveiligheid voldoende geborgd is. Meer specifiek wenst de rekenkamercommissie meer inzicht te krijgen in de wijze waarop taken, verantwoordelijkheden en bevoegdheden zijn verdeeld en op welke wijze dit invloed heeft op de besluitvorming. We richten ons dus niet op het bestaan en de werking van specifieke organisatorische, procesmatige of technische beveiligingsmaatregelen.

1.2. Doel en onderzoeksvraag

Het doel van het onderzoek is het verkrijgen van inzicht in de rollen die de verenigde vergadering (VV) als algemeen bestuur van HHR en het college van dijkgraaf en hoogheemraden (D&H) als dagelijks bestuur van HHR vervullen ten aanzien van informatiebeveiliging. De focus ligt daarbij op de wijze waarop de Plan-Do-Check-Act-cyclus (PDCA-cyclus) wordt gevolgd in het samenspel tussen de drie gremia (respectievelijk de politieke, bestuurlijke en ambtelijke organisatie). De RKC van HHR heeft hiervoor de volgende hoofdvraag geformuleerd:

Hoofdvraag: *Is het bestuur van het hoogheemraadschap van Rijnland in control ten aanzien van informatieveiligheid?*

[2] Onder informatieveiligheid verstaan we: "Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen." Bron: Baseline Informatiebeveiliging Overheid. Met de termen informatieveiligheid en informatiebeveiliging worden door elkaar heen gebruikt en hebben dezelfde betekenis binnen dit rapport.

De deelvragen zijn door de RKC als volgt geformuleerd:

- **Organisatorische inrichting**: Is het de drie gremia duidelijk waar de verantwoordelijkheden en bevoegdheden liggen van elk van de drie gremia met betrekking tot de PDCA-cyclus (planvorming, uitvoering, controle en evaluatie, bijstellen) om de afgesproken informatieveiligheid te bereiken? Is de aangetroffen organisatorische inrichting een goede?
- **PDCA, Risicomanagement en Rapportage**: Werkt er een PDCA-cyclus ten aanzien van informatieveiligheid? Worden per onderdeel van PDCA de goede acties uitgevoerd en besluiten genomen door elk gremium, conform de organisatorische inrichting? Een punt van aandacht hierbij is het risicomanagement: Is het vaststellen van de risicobereidheid en het managen ervan onderdeel van elke stap van de PDCA-cyclus? Een ander punt is de rapportage (controle en evaluatie): vindt die op een goede wijze plaats?

1.3. Opzet

Bij de opzet van het onderzoek hebben we het proces opgedeeld in vijf stappen. Deze stappen treft u aan in Figuur 1.

B

Aanpak op hoofdlijnen

Figuur 1: Proces uitvoering onderzoek

De onderzoeksdata zijn verzameld door middel van het uitvoeren van een documentstudie en het afnemen van interviews. In Bijlage 1 treft u een overzicht van de ontvangen en gebruikte documentatie aan, in Bijlage 2 een lijst van deelnemers aan de interviews.

1.4. Leeswijzer

Deze Nota van Bevindingen vormt het door Berenschot opgestelde eindrapport. In *hoofdstuk 2* van deze nota beschrijven we de taken en bevoegdheden van de relevante organen van HHR die binnen de scope van de opdracht vallen en in *hoofdstuk 3 tot en met 6* van deze nota delen we achtereenvolgens onze bevindingen ten aanzien van de onderwerpen organisatorische inrichting, rapportage, risicomanagement en de werking van de PDCA-cyclus.

2. Context informatiebeveiliging binnen HHR

In dit hoofdstuk beschrijven we eerst op hoofdlijnen de context waarbinnen we het onderzoek hebben uitgevoerd en het perspectief van waaruit we naar de organisatie kijken.

1.5. Organisatie van informatiebeveiliging binnen HHR

HHR deelt de ICT- en informatievoorzieningen binnen het waterschap met het hoogheemraadschap van Schieland en Krimpenerwaard (HHSK). Deze keuze is gemaakt vanuit de overtuiging dat dit voordelen biedt vanuit het perspectief kosteneffectiviteit en -efficiëntie. Hierbij heeft men de keuze gemaakt om deze samenwerking dan ook door te trekken in een gezamenlijk informatiebeveiligingsbeleid en een gezamenlijke invulling van de functies Chief Information Officer (CIO) en Chief Information Security Officer (CISO). Besluitvorming van onderwerpen die beide organisaties gezamenlijk raken, worden voor zover mogelijk afgehandeld in een overleg dat periodiek tussen beide secretaris-directeuren van de waterschappen plaatsvindt (het zogeheten 2SD-overleg).
Momenteel is HHR bezig met het uitvoeren van de visie *Op weg naar een datagestuurd Rijnland – visie op de digitale transformatie*[3]. Rijnland heeft er in dat kader voor gekozen een digitale transformatie door te gaan. De besluitvorming en kaders hiervan zijn vastgesteld door de VV in een besluitnota in 2021. In deze visie worden drie aandachtsgebieden onderscheiden, namelijk:

1. We implementeren digitale ontwikkelingen als die tot meer effectiviteit of efficiëntie leiden.
   Hoe digitaliseren we ons werk?
2. We zijn alert op informatiebeveiliging, privacy en ethiek.
   Hoe blijven we digitaal weerbaar?
3. De relatie met de omgeving verandert met impact op de dienstverlening en samenwerking.
   Hoe blijven we in verbinding met de omgeving?

Deze transformatie is momenteel nog volop in ontwikkeling en heeft de afgelopen tijd geleid tot grote veranderingen binnen de organisatie, waaronder op het gebied van informatiebeveiliging. De documenten die we hebben ontvangen en de informatie die we hebben opgehaald tijdens de interviews bevestigen dit beeld grotendeels. Zo zien we dat de organisatie op veel vlakken vooruitgang boekt op het gebied van de inrichting van informatiebeveiliging. Men is heel bewust bezig met het bestendigen van een goede implementatie van het Three Lines of Defense model[4] en met risicogebaseerd sturen. Bovendien merken we uit de interviews op dat zowel binnen de ambtelijke organisatie als bij D&H en de VV aandacht is voor het onderwerp.
Hoewel de informatie uit de rapportages op dit moment nog vrij technisch en operationeel gericht is, zien we een duidelijke visie op waar men in de organisatie naar toe wenst te bewegen.
Deze visie zien we niet alleen terug in de relatie tussen de verschillende lagen van de ambtelijke organisatie, maar ook in de rapportage richting de VV.

[3] Visie *Op weg naar een datagestuurd Rijnland – visie op de digitale transformatie*

[4] Het Three Lines of Defense model is een model dat wordt gebruikt voor de inrichting van een organisatie. Het model onderscheidt drie lagen binnen de organisatie die elk een functie vervullen in het identificeren, adviseren, en mitigeren van (informatiebeveiligings-)risico's binnen organisaties. Een uitgebreide toelichting op dit model is bijvoorbeeld te vinden op de website van het Instituut van Interne Auditors Nederland: https://www.iia.nl/kenniscentrum/vaktechnische-publicaties/publicatie/three-lines-model-updated---nl.
In hoofdstuk 3 staat een nadere uitwerking van het Three Lines of Defense model binnen HHR.

1.6. Taken, verantwoordelijkheden en bevoegdheden

Binnen dit onderzoek hebben we ons primair gericht op het onderzoeken hoe de verschillende organen binnen HHR zich tot elkaar verhouden ten aanzien van informatiebeveiliging. Daarbij hebben we ons specifiek gericht op de wijze waarop de VV, D&H en de ambtelijke organisatie zich tot elkaar verhouden. In dit hoofdstuk beschrijven we in algemene zin welke taken en verantwoordelijkheden zij hebben.

Algemeen bestuur (VV)

De VV stelt het beleid van het waterschap vast. Het controleert ook of D&H dat beleid goed uitvoert. Met andere woorden: het waterschap voert een kaderstellende en controlerende taak uit. Deze taken hebben zij ook ten aanzien van beleid en controle op informatieveiligheid.
Onder de kaderstellende rol valt het vaststellen van de begroting en de jaarrekeningen en het nemen van besluiten waarin kaders worden gesteld waarbinnen D&H kan handelen. Hiervoor beschikt de VV over de nodige instrumenten, zoals: het vaststellen van de begroting en de jaarrekening, verordeningen maken, het vaststellen van plannen, of het indienen van moties.
Onder de controlerende rol valt de controle of beleid en uitvoering van D&H past binnen de gestelde kaders. Hieronder vallen bijvoorbeeld het periodiek ontvangen van informatie waaronder de Buraps, nota's, accountantsverklaringen en de mogelijkheid tot het stellen van vragen.
In de praktijk is het voor de leden van de VV noodzakelijk om prioriteiten te stellen ten aanzien van de vele uitdagingen waar waterschappen mee te maken krijgen. Op basis van deze prioritering zullen vervolgens keuzes gemaakt worden op welke wijze de kaderstellende en controlerende rol wordt uitgevoerd.

Dagelijks bestuur (D&H)

D&H is verantwoordelijk voor de voorbereiding en uitvoering van het beleid. Het D&H is belast met de dagelijkse aangelegenheden van het waterschap. Daarnaast draagt D&H de verantwoordelijkheid om de VV te ondersteunen in de voorbereiding op de besluitvorming.
Mede op basis van de input die we hebben verzameld tijdens de interviews, begrijpen we dat D&H ten aanzien van informatiebeveiliging zich in de praktijk voornamelijk bezighoudt met het formuleren van een visie en de ambities die vervolgens aan de VV worden voorgelegd ter besluitvorming.

Ambtelijke organisatie

Onder de ambtelijke organisatie verstaan we de (operationele) organisatie die onder leiding van de secretaris-directeur staat. In het kader van dit onderzoek betekent dit dat we ons richten op de belangrijkste functies en rollen die betrokken zijn bij informatiebeveiliging. We maken daarbij geen onderscheid tussen kantoorautomatisering of operationele technologie. Meer specifiek richten we ons in het kader van dit onderzoek op de hoogste functies op alle drie de lijnen uit het Three Lines of Defense model, zoals de secretaris-directeur, het hoofd bedrijfsvoering, de CIO, CISO en de belangrijkste IV-adviseurs.

3. Bevindingen organisatorische inrichting

In dit hoofdstuk treft u de belangrijkste bevindingen aan ten aanzien van de sturing op informatieveiligheid door Rijnland. In de navolgende paragrafen beschrijven we per onderwerp wat onze beelden zijn op basis van de ontvangen documenten en gevoerde gesprekken.
Omdat de scope van het onderzoek voornamelijk is gericht op het samenspel tussen de ambtelijke organisatie, D&H en de VV, beperken we ons tot het beschrijven van deze functies en van de functies CIO en CISO.

1.7. Organisatorische inrichting

Algemeen bestuur (VV)

De VV is verantwoordelijk voor het vaststellen van het beleid. Daarnaast controleert de VV of D&H het beleid ook op de juiste wijze uitvoert. Binnen de VV is er een commissie Bestuur, Organisatie en Dienstverlening (BOD) die zich onder meer bezighoudt met de informatievoorziening binnen HHR en het waarborgen dat informatiebeveiliging goed is ingericht.
Uit de ontvangen documenten van Rijnland zien we geen expliciete rol terug voor de VV. Het Strategisch beleid Informatiebeveiliging 2022 – 2025 (versie 0.5 – oktober 2022) beschrijft enkel taken en verantwoordelijkheden voor de ambtelijke organisatie en D&H. Uit het interview met diverse leden van de VV kwam ook naar voren dat informatieveiligheid niet specifiek in de portefeuilles van de leden zit. De informatiebehoefte en kaderstellende functie vanuit de VV werd dan ook als volgt samengevat door de aanwezigen bij de interviews:

- D&H formuleert de ambities. Deze ambities worden voorgelegd aan de VV en de VV stemt hiermee in.
- De VV wil vooral weten dat het geregeld is door de ambtelijke organisatie, maar hoeft niet op de details betrokken te worden. De VV controleert met name of iedereen binnen D&H en de ambtelijke organisatie in staat is zijn/haar rol te vervullen. Men heeft daarbij veel vertrouwen in D&H en de ambtelijke organisatie.
- De rol voor de VV is met name aanwezig op het moment dat blijkt dat er onvoldoende middelen zijn om de geformuleerde ambitie te behalen. De VV besluit in die gevallen of er aanvullende middelen vrijgemaakt kunnen worden.
- Er wordt gerapporteerd aan de VV over de stand van zaken. Tegelijkertijd wordt opgemerkt door enkelen dat dit meer ter kennisgeving wordt aangenomen, dan dat er inhoudelijk over gesproken wordt.

- Het onderwerp informatieveiligheid is typisch een onderwerp waarvoor sterk gesteund wordt op de vakdeskundigen op dit gebied. Tijdens het interview met enkele leden van de VV werd door verschillende leden aangegeven dat zij zelf over onvoldoende inhoudelijke kennis beschikken om inhoudelijk te toetsen of informatieveiligheid voldoende geborgd is. Een van de leden merkte daarbij op dat men het ook ziet als een randvoorwaarde die voldoende gewaarborgd moet zijn. Tegelijkertijd geven enkele leden ook aan dat zij het toenemende belang van informatieveiligheid herkennen en hierover graag het gesprek willen voeren. Wel is men nog op zoek naar de wijze waarop dit zou moeten plaatsvinden.

Dagelijks bestuur (D&H)

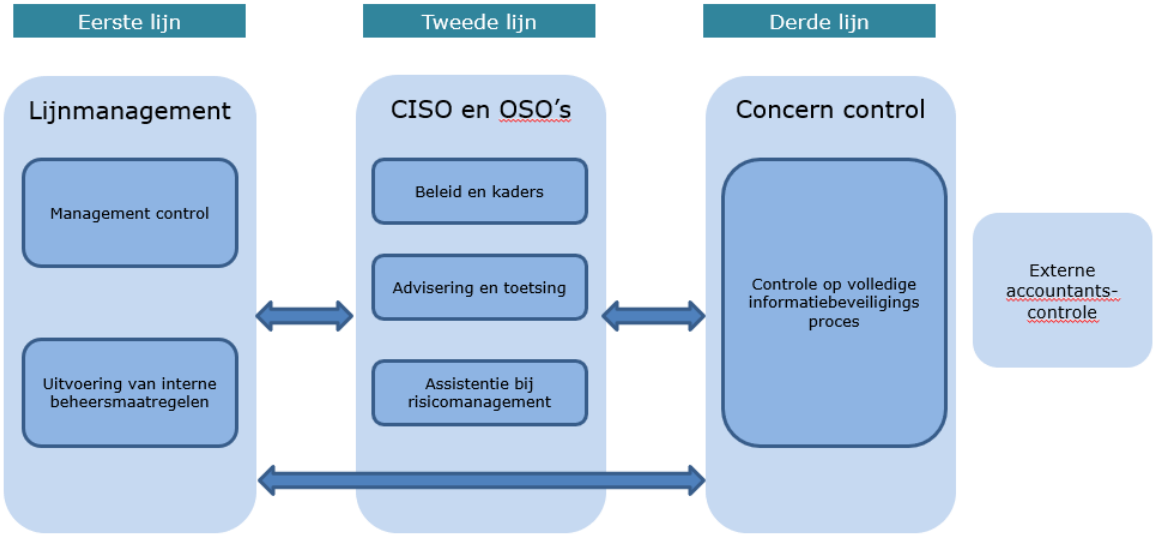
D&H is (eind-)verantwoordelijk voor de voorbereiding en uitvoering van het beleid van HHR.
Uit de documentatie is op één onderdeel de rol van D&H af te leiden. In het Strategisch beleid Informatiebeveiliging 2022 – 2025 wordt de rol van de hoogheemraad omschreven als belast met de portefeuille voor informatieveiligheid. Het valt echter niet af te leiden wat 'belast met de portefeuille' concreet betekent.
Uit de interviews is naar voren gekomen dat de hoogheemraad deze rol als volgt invult. De hoogheemraad acht zichzelf eindverantwoordelijk voor het onderwerp en houdt zich voornamelijk bezig met de strategische vraagstukken op dit thema en of er voldoende mensen en middelen binnen de organisatie aanwezig zijn om de ambities te verwezenlijken. Om grip te krijgen op de huidige stand van zaken heeft de hoogheemraad onder meer de huidige stand van zaken in kaart gebracht en vervolgens een koersnota geschreven. De koersnota is ter kennisname aangeboden aan de VV. De werkzaamheden van de hoogheemraad zijn dan ook voornamelijk gericht op:

- Het ondersteunen van de ambtelijke organisatie met voldoende mensen en middelen. Bijvoorbeeld door te zorgen dat posities vervuld zijn.
- Het realiseren van strategische ambities voor de gehele digitale transitie in de brede zin.
- Het monitoren in hoeverre deze ambities daadwerkelijk behaald worden gedurende de periode en het informeren van de VV hierover.

Ambtelijke organisatie

De IT-voorziening wordt door HHR gedeeld met het hoogheemraadschap van Schieland en Krimpenerwaard (HHSK). HHR werkt op het gebied van informatiebeveiliging dan ook nauw samen met HHSK en ze zorgen gezamenlijk voor voldoende personeel en het vaststellen van beleid.

- Uit het Strategisch beleid Informatiebeveiliging 2022 – 2025 zien we een duidelijke organisatiestructuur terugkomen die is ingericht op het Three Lines of Defense model. In Figuur 2 treft u de inrichting volgens dit model aan. In dit model is het lijnmanagement (1ste lijn) verantwoordelijk voor de veiligheid van systemen en informatie. De CISO en de operationeel security officers (OSO's) (2de lijn) ondersteunen de organisatie, en meer specifiek het lijnmanagement, door het geven van adviezen over dreigingen, opstellen van beleid en het stellen van kaders. Ook ondersteunen zij bij het inrichten van systemen rondom risicomanagement. Tot slot worden er periodiek audits uitgevoerd door interne en externe auditors (3de lijn). Zij controleren het volledige informatiebeveiligingsproces en het samenspel tussen de 1ste en 2de lijn.



Figuur 2: Three Lines of Defense model HHR (bron: informatiebeveiligingsbeleid HHR)

Uit de interviews komt naar voren dat indien beleid en kaders moeten worden vastgesteld die op zowel HHR als HHSK van toepassing zijn, dit altijd plaatsvindt via het periodieke 2SD-overleg. Dit overleg vindt plaats tussen de secretaris-algemeen directeur van HHR en de secretaris-algemeen directeur van HHSK. Daarbij wordt wel opgemerkt dat uiteindelijk de VV en D&H verantwoordelijk zijn voor het vaststellen van het beleid en benodigde financiering. Ook de keuze om volwassenheidsniveau 4 te behalen met betrekking tot de BIO wordt genoemd als voorbeeld van een besluit dat genomen wordt door de VV en D&H.
De iRaad geeft bindend advies aan de directie over het Strategisch beleid Informatieveiligheid en informatiebeveiligingsplannen en het vaststellen van tactisch informatiebeveiligingsbeleid.[5]

Samenvattend

De kaderstellende rol van de VV uit zich met name in besluitvorming over voorstellen die worden voorbereid door D&H. De voorstellen die worden gedaan, richten zich primair op het stellen van ambities en de daarvoor benodigde middelen. Daarbij wordt informatiebeveiliging veelal als randvoorwaardelijk beschouwd. Als gevolg hiervan concentreert de besluitvorming ten aanzien van informatiebeveiliging zich veelal binnen de ambtelijke organisatie. D&H en VV vertrouwen bij het nemen van besluiten primair op de directie van de ambtelijke organisatie. Dit vertrouwen komt deels voort uit de opvatting van VV dat informatieveiligheid een operationeel onderwerp is dat ook voornamelijk bij de ambtelijke organisatie thuishoort. Anderzijds geeft men ook aan dat de inhoudelijke kennis van het onderwerp beperkt is en men het lastig vindt om beslissingen te nemen.

[5] De iRaad bestaat uit verschillende stakeholders van zowel HHR als HHSK, waaronder: Manager I&D, enterprise architect, strategisch adviseur directie, het afdelingshoofd Bestuur, Informatie, en Juridisch Advies vanuit HHSK, de CISO's van beide organisaties en een Business Relationship Manager.

4. Bevindingen rapportages

We hebben inzicht gekregen in de verschillende typen rapportages die op verschillende niveaus gedeeld worden binnen HHR. Een beschrijving van de verschillende rapportages treft u in deze paragraaf aan.

Algemeen bestuur (VV)

De belangrijkste rapportages die de VV ontvangt inzake informatiebeveiliging zijn de jaarverslagen waarin men rapporteert over de risico's, maar ook de periodieke Buraps. De Buraps bevatten standaard een onderdeel Bestuur, Organisatie, en Dienstverlening (BOD) waar ook gerapporteerd wordt over informatieveiligheid. In de Voorjaarsburap 2022 was hierover het volgende opgenomen:

> *De ingezette lijn om de cyberweerbaarheid van onze waterschap te verhogen heeft geleid tot de operationalisering van een Security Operations Center (SOC) per februari 2022 dat ons ondersteunt bij mogelijke beveiligingslekken en cyberdreigingen. Ook zijn de voorbereidingen voor het hybride werken gestart met zowel aanpassingen aan het pand als aanschaf en aanleg van ICT-voorzieningen om de medewerkers een hybride werkplek te geven (monitor, dockingstation, laptops). De hardware leveringen voor datacenter en Wifi op de buitenlocaties zijn door de chiptekorten tot april 2022 uitgesteld. Wij verwachten echter dat we alles nog in 2022 kunnen installeren. Daarnaast wordt een Meerjarenonderhoudsplan (MJOP) opgesteld voor alle assets in eigendom (buiten het primaire proces). Dit om inzicht te verkrijgen in achterstallig onderhoud en planmatig te kunnen werken. De verwachting is dat we een inhaalslag moeten maken. Ook is een begin gemaakt om de fysieke beveiliging van Rijnlandse objecten te verbeteren.*
> **Bron: Voorjaarsburap 2022**

Daarnaast ontvangt het algemeen bestuur ook nog informatie en rapportages op ad hoc basis. Meestal betreffen dit zogeheten TKN-memo's. De aanleiding hiervoor kan zijn dat D&H reden ziet om de VV proactief te informeren over een onderwerp of de VV heeft specifieke vragen gesteld over een bepaald onderwerp. Voorbeelden van dergelijke ad hoc rapportages zijn bijvoorbeeld het Memo gedeeld door D&H over cyberincidenten van 6 april 2022[6].

Dagelijks bestuur (D&H)

D&H draagt eindverantwoordelijkheid voor de staat van informatieveiligheid binnen het waterschap. Het is dus van belang dat het voldoende geïnformeerd wordt over het dreigingslandschap, de risico's en de lopende projecten om maatregelen te implementeren om de risico's op de juiste wijze aan te pakken.
De wijze van rapporteren aan de portefeuillehouder binnen D&H wordt in het Strategisch beleid Informatiebeveiliging 2022 – 2025 expliciet gemaakt.
Zo wordt de portefeuillehouder in ieder geval ieder half jaar op de hoogte gebracht van de algemene staat van informatieveiligheid binnen het waterschap.
Uit de interviews komt naar voren dat rapporteren aan de portefeuillehouder in veel gevallen gebeurt tijdens (informele) voortgangsoverleggen vanuit verschillende niveaus binnen de ambtelijke organisatie. Deze overleggen vinden op verschillende niveaus binnen de ambtelijke organisatie plaats.

[6] https://rijnland.bestuurlijkeinformatie.nl/Reports/Document/9e95d0fd-22a8-45f4-8a2c-860781ff8251?documentId=4790cd0e-9878-47ae-874f-3381ef44a479

Ambtelijke organisatie

Met behulp van een dashboard hebben systeemeigenaren actueel inzicht in de status van maatregelen op het gebied van informatiebeveiliging. De OSO's controleren minimaal maandelijks de status van de maatregelen op afwijkingen. Bij een langer durende afwijking (dat wil zeggen een afwijking die 2 maanden of langer duurt) nemen zij contact op met de systeemeigenaren om de achterstand te bespreken en verbetermaatregelen door te spreken.

Er wordt per kwartaal gerapporteerd aan de directie. In de bespreking die de directie en CISO elk kwartaal voeren, worden het dreigingsbeeld/de risico's, de actuele status en de voortgang van de verbeterplannen besproken teneinde de lijnverantwoordelijkheid te borgen.

Tot slot vinden er maandelijkse rapportages plaats over de informatiebeveiligingsincidenten en informatiebeveiligingsrisico's. Deze worden elk kwartaal verstrekt aan de iRaad. Tijdens de iRaad vergadering worden de uitzonderingen en afwijkingen in relatie tot kaders en projecten voor informatieveiligheid besproken. Alleen wanneer er hoog-risico incidenten dan wel dreigingen zijn, wordt de iRaad tussentijds geïnformeerd.

5. Bevindingen risicomanagement

Risicomanagement vormt de basis van informatiebeveiliging binnen Rijnland. Een optimaal niveau van informatiebeveiliging wordt bereikt door een risicoanalyse en daaropvolgend een zorgvuldige afweging van de strategie hoe daar mee om te gaan. Het vaststellen van risicobereidheid is een belangrijke onderdeel van risicomanagement. Keuzes die gemaakt worden ten aanzien van risicobereidheid hebben potentieel een enorme impact op de kosten die worden gemaakt ten aanzien van het nemen van maatregelen. Zo zal in de regel een lage risicobereidheid leiden tot hoge kosten ten aanzien van het nemen van informatiebeveiligingsmaatregelen, maar zal de kans op onvoorziene uitgaven door incidenten redelijkerwijs klein zijn. Een hoge risicobereidheid kan daarentegen tot het omgekeerde leiden.

Algemeen bestuur (VV)

Om de kaderstellende rol optimaal uit te kunnen voeren heeft de VV er baat bij om risicomanagement in de volle breedte te bezien. Wanneer een volledig beeld bestaat van de risico's is het beter mogelijk om kaders vast te stellen waarbinnen D&H kan opereren.
Afgaande op de informatie uit de onderzochte rapportages blijkt dat de IT-voorzieningen worden beschreven onder de kop *Bestuur, Organisatie & Dienstverlening (BOD)*. De informatie in deze rapportages betreft voornamelijk de voortgang van de implementatie van te nemen maatregelen op het gebied van informatiebeveiliging.
Op basis van de aangeleverde documentatie en de interviews lijkt de rol van de VV ten aanzien van risicomanagement zeer beperkt. Tijdens het interview met de VV valt op dat men aangeeft onvoldoende thuis te zijn in de informatiebeveiligingsmaterie en het te beschouwen als integraal onderdeel van de bedrijfsvoering en hiervoor te vertrouwen op D&H en de ambtelijke organisatie. Tegelijkertijd zijn er, op het moment van onderzoek, ook signalen dat men in sommige gevallen graag meer inzicht zou willen hebben in concrete risico's en de te nemen maatregelen.
Ook D&H en (de directie van) de ambtelijke organisatie geven aan te zoeken naar middelen om de VV beter te kunnen informeren en in staat te stellen om zijn kaderstellende en controlerende rol beter uit te kunnen voeren.
Tegelijkertijd hebben we uit de onderzochte documentatie kunnen afleiden dat de VV enkele specifieke kaders heeft vastgesteld op het onderdeel risicomanagement bij informatiebeveiliging. Zo is tijdens de interviews naar voren gekomen dat de VV heeft besloten dat HHR minimaal aan volwassenheidsniveau 4 dient te voldoen met betrekking tot informatiebeveiliging en implementatie van de BIO. Dit volwassenheidsniveau houdt in dat vereiste beheersmaatregelen worden vastgesteld op basis van risicoanalyses en dat de effectiviteit van de maatregelen periodiek worden getoetst aan het risicoprofiel van de organisatie.

Dagelijks bestuur (D&H)

Zowel uit de documentatie als uit de interviews is geen nadrukkelijke rol voor D&H naar voren gekomen op het gebied van risicomanagement. De hoogheemraad geeft te kennen dat risicomanagement meer impliciet onderdeel uitmaakt van gesprekken en besluiten.
Het besluit tot volwassenheidsniveau 4, zoals hierboven vermeld, geeft overigens wel blijk van het belang dat wordt toegekend aan risicomanagement. Deze ambitie, ingezet door D&H en aangescherpt

aan de hand van input uit de ambtelijke organisatie, laat zien dat risicomanagement in kaderstellende zin naar voren komt bij D&H.

Ambtelijke organisatie

Binnen de ambtelijke organisatie zien we dat de implementatie van risicomanagement en daarmee een risicogebaseerde sturing het meest terugkomt.
De kaders voor het toepassen van risicomanagement staan expliciet beschreven in het Strategisch beleid Informatiebeveiliging. Daarin wordt risicomanagement op drie niveaus beschreven: Organisatie, Objecten, en BIO controls. Daarnaast beschrijft het beleid tevens het risicomanagementproces.
Er zijn verschillende processen die doorlopen kunnen worden om inzicht te krijgen in de risico's van informatievoorzieningen. Zo voert de organisatie in beginsel voor alle assets een Business Impact Analyse (BIA) uit. Indien hiervoor aanleiding bestaat, wordt daarnaast in specifieke gevallen nog een Data Protection Impact Assessment (DPIA) en/of diepgaande risicoanalyse uitgevoerd. De resultaten van deze risicoanalyses worden tevens gedeeld met de CISO en/of Functionaris Gegevensbescherming (FG). Zoals beschreven in *hoofdstuk 4 - Bevindingen rapportages* worden er periodiek geaggregeerde rapportages besproken met de directie zodat zij, waar nodig, kan bijsturen.

6. Bevindingen werking PDCA-cyclus

Uit voorgaande paragrafen is reeds een en ander naar voren gekomen over de werking van de Plan-Do-Check-Act-cyclus, ook wel de Deming-cirkel genoemd. In feite is de werking van de PDCA-cyclus ook een effect van de wijze waarop de organisatie is ingericht op het gebied van governance, risicomanagement en rapportages.

Algemeen bestuur (VV)

Als we kijken naar de VV, dan bleek eerder reeds dat zij betrokken is bij ambitieformulering op het gebied van informatiebeveiliging. Relateren we dit aan de PDCA-cyclus, dan kunnen we daarmee in elk geval concluderen dat zij zich betrokken voelt bij de (strategische) planfase. Ook wil zij op de hoogte zijn van uitvoeringsproblematiek in de do-fase. In de check/act-fase zien we minder betrokkenheid. Zo werd door de geïnterviewde leden aangegeven dat het ontbreekt aan de juiste kennis om vragen te stellen over rapportages. Dit zien we ook terug in de openbare informatie van de vergaderingen van de VV. In een steekproef van de notulen zien we het onderwerp informatieveiligheid nauwelijks naar boven komen en zien we ook dat overige informatie rondom het onderwerp vooral ter kennisname behandeld wordt, in de zogeheten TKN-memo's. Dit is in lijn met dat wat de VV-leden zelf aangaven over hun controlerende rol en beperkt daarmee de rol van de VV in de check/act fase. Bovendien is het goed uitvoeren van een controlerende rol ook afhankelijk van de kwaliteit van de informatie in de rapportages.

Dagelijks bestuur (D&H)

Zowel uit de documentatie als de interviews is gebleken dat de rol van D&H, vooral via de portefeuillehouder, nadrukkelijk aanwezig is op het gebied van plan (ambitiebepaling, planvorming) en do (uitvoeringsproblematiek). Daarnaast neemt D&H kennis van de check door middel van terugkoppelingen uit de organisatie en externe audits. Op basis hiervan kijken zij met de ambtelijke organisatie of bijstelling van plannen noodzakelijk is. Ook hier geldt wederom dat het vertrouwen in de ambtelijke organisatie ertoe leidt, dat de betrokkenheid van D&H beperkt is tot het strategisch niveau en met name een focus heeft op ambitiebepaling.

Ambtelijke organisatie

De ambtelijke organisatie is nadrukkelijk aan het groeien in volwassenheid. Bij een groei in volwassenheid van het managementsysteem voor informatiebeveiliging, hoort ook een groei in de mate waarin de PDCA-cyclus gebruikt wordt. We constateren op basis van de interviews en de documentatie dat hier goede stappen in gezet worden. Zo is men de afgelopen jaren steeds meer gestructureerd aan de slag gegaan met de verbetermaatregelen die geconstateerd werden. Niet altijd is door ons overigens een directe koppeling te maken tussen verbetermaatregelen uit audits en plannen die nu uitgevoerd worden, mede in relatie tot de rapportages die daaruit volgen richting bestuur.

Bijlage I. Ontvangen documentatie

- 20221005 Onderzoeksvoorstel informatieveiligheid RKC Rijnland (def).pdf
- 22.074908 Risicobeoordeling PA back up infrastructuur.pdf
- 2207 Procesbeschr HHSK.pdf
- 2207 VVT HHR.pdf
- 2207 VVT HHSK.pdf
- Anti skimming kaartje.pdf
- Auditrapport Integrale BIO_AVG audit (1).pdf
- Auditrapport Integrale BIO_AVG audit HHR (1).pdf
- Auditrapport Integrale BIO_AVG audit HHR (1).pdf
- BELEID EIGENAARSCHAP 1.6.pdf
- Bliksem BIA Data Platform - KNMI.pdf
- kaartje_informatieveiligheid_highres.pdf
- Koffiescherm_informatiestromen.png
- Koffiescherm_koffiehalenschermopslot.png
- Krant-van-de-veiligheid.pdf
- KT werkblad - Vodafone infra aandachtspunt.xlsm
- Procesflow risico-analyse.PNG
- Rapport IB meldingen DIG-1184-004 202204 (1).pdf
- Rapport IB meldingen DIG-1184-004 202204.pdf
- Rapport IB meldingen DIG-1184-004 202206.pdf
- Rapport IB meldingen DIG-1184-004 202207.pdf
- Rapport IB meldingen DIG-1184-004 202208.pdf
- Rapport IB risicos DIG-1184-004 juli 2022.pdf
- Rapport IB risicos DIG-1184-004 juni 2022.pdf
- Rapport IB risicos DIG-1184-004 mei 2022.pdf
- Rapportage_HoogheemraadschapvanRijnland_VR2022126197_september_2022_v1.pdf
- RE Voorbereiding startbijeenkomst RKC onderzoek informatieveiligheid.msg
- Scores DataQuiz intern.JPG
- Strategisch beleid Informatiebeveiliging 2022 - 2025.docx (versie 0.5 / oktober 2022)
- VERTROUWELIJK (Sectorrapportage BIO en AVG audits 2021 2022 v1.0def).pdf
- VERTROUWELIJK (Sectorrapportage BIO en AVG audits 2021 2022 v1.0def).pdf
- Werkinstructie BIA v1.4.pdf

Bijlage II. Deelnemers interviews

*Het onderzoek is uitgevoerd ten tijde van de vorige bestuursperiode.

Interview 1: inhoudelijk experts ambtelijke organisatie	Adviseur Informatievoorziening en Informatiebeveiliging a.i. CISO Manager I&D.
Interview 2: management ambtelijke organisatie	Secretaris-algemeen directeur Hoofd bedrijfsvoering
Interview 3: portefeuillehouder D&H	Thea Fierens – Hoogheemraad
Interview 4: leden van de VV*	Bernard Revet 50PLUS Frank Pardaan VVD Jaap van Oeveren VVD Ineke van Steensel VVD Roberto Schols 50PLUS René Roorda CU_SGP Marco Kastelein CDA (hoogheemraad) Jan de Vries AB (hoogheemraad) Piet vd Poel AB John vd Slot AB Waldo von Faber Water Natuurlijk (hoogheemraad) Thea Fierens PvdA (hoogheemraad) Enrico van Dijk Water Natuurlijk *Tevens aanwezig bij het gesprek:* Secretaris-algemeen directeur Hoofd bestuurszaken