

# Bestuursvoorstel



Voorstelnummer: 2018-003

Houten, 30 maart 2018

---

## Onderwerp:

Rekenkameronderzoek Quickscan Digitale Veiligheid.

---

## Beslispunten:

- 1) Kennis te nemen van de resultaten van het onderzoek van de rekenkamercommissie met betrekking tot borging en verantwoording ten aanzien van digitale veiligheid.
- 2) In te stemmen met de aanbevelingen van het rapport.

---

## Samenvatting:

Het rekenkameronderzoek laat zien dat de wisselwerking tussen het Algemeen Bestuur en het Dagelijks Bestuur wat betreft de digitale veiligheid van HDSR beperkt is. Het onderwerp staat beperkt op de bestuurlijke agenda en wordt veelal reactief behandeld door het dagelijks bestuur.

De staat van de wisselwerking en de beperkte materiekkennis ten aanzien van digitale veiligheid binnen het Algemeen Bestuur bemoeilijken de controlerende functie van het Algemeen Bestuur op dit onderwerp.

De expliciete verantwoording wordt als onvoldoende inzichtelijk ervaren door het Algemeen Bestuur. Dit werkt niet stimulerend voor het vertrouwen in de mitigatie ten aanzien van digitale dreigingen door HDSR.

De borging en verantwoording vinden met name plaats in de ambtelijke organisatie, waar met name kennis over de digitale veiligheid aanwezig is, specifiek bij CISO. Hier wordt zowel door de ambtelijke organisatie als door het bestuur sterk op geleund.

Het onderzoek constateert dat HDSR structureel en zorgvuldig risicoanalyses uitvoert op het gebied van informatiebeveiliging en daarbij concreet de te nemen maatregelen benoemt. Hierbij baseert HDSR zich met name op wettelijke kaders en sectorale afspraken zoals het BIWA-normenkader.

Het inzicht in de digitale dreigingen en maatregelen beperkt zich echter tot de ambtelijke organisatie.

---

## Aanbevelingen:

Op basis van de bevindingen en de conclusies zijn er een aantal concrete tips en aanbevelingen geformuleerd voor het algemeen bestuur.

### 1. Beleidsmatige kaders

- HDSR gebruikt met name de landelijke normen uit de BIWA als beleidskader. Het is verstandig om standaarden uit het veld te gebruiken, echter er kunnen goede redenen zijn (op basis van een risicoanalyse) om van de BIWA af te wijken. Denk bijvoorbeeld aan een waterschap dat de ict-dienstverlening voor meerdere waterschappen uitvoert; de impact van uitval van ict-dienstverlening is daarmee groter. Het kan zijn dat daarom meer maatregelen wenselijk zijn. Vandaar dat de stelling om de BIWA te volgen dus een stevigere onderbouwing behoeft.
- Het algemeen bestuur geeft aan over onvoldoende kennis te beschikken om een kaderstellende rol goed te vervullen. Dat is ook niet vreemd gezien de complexiteit van het onderwerp. Uiteraard is het Algemeen Bestuur van HDSR niet het enige bestuur dat met dit vraagstuk speelt. Je zou kunnen leren van

andere besturen (bijvoorbeeld van waterschappen) om zo beter invulling te kunnen geven aan de kaderstellende taak.

- HDSR beschikt over een informatiebeveiligingsbeleid, echter deze is niet door het bestuur vastgesteld. Om het vertrouwen van het bestuur op dit onderwerp te verstevigen zou het goed zijn om het beleid (of de hoofdlijnen hiervan) door het bestuur te laten vaststellen.

## 2. Inzicht in risico's

- De ambtelijke organisatie is continu bezig met het verbeteren van de risicoanalyse methodiek. Het is raadzaam om deze ontwikkeling door te zetten, zeker gezien het toenemende belang van ict in de processen van het hoogheemraadschap.

- HDSR werkt met twee verschillende risicoanalyse methodieken: een losse voor digitale veiligheid en een organisatiebrede analyse. De twee analyses staan niet helemaal los van elkaar, maar de relatie tussen beide analyses zou nog verstevigd kunnen worden. Daarnaast wordt de risicoanalyse op het gebied van digitale veiligheid niet breed gedeeld in de verantwoordingsketen. Het is aan te bevelen om ook het bestuur hierin met regelmaat mee te nemen, al is het op wat abstracter niveau in verband met geheimhouding.

## 3. Verantwoording ten aanzien van digitale veiligheid en digitale bedreigingen

- Maak afspraken tussen Dagelijks Bestuur en Algemeen Bestuur over een periodieke verslaglegging. Besteed daarbij aandacht aan de wensen over inhoud en vorm van het Algemeen bestuur ten aanzien van die rapportage. Dat helpt het AB met haar controlerende taak, wat weer bijdraagt aan het vertrouwen in het Dagelijks bestuur en de ambtelijke organisatie op dit onderwerp.

- In de ambtelijke organisatie wordt sterk geleund op het werk van de CISO; het zou voor de borging van dit belangrijke onderwerp goed zijn als:

- o verantwoordelijkheden breder in de organisatie belegd worden. Dit begint met bewustwording bij iedereen dat digitale veiligheid een integraal onderdeel van de dagelijkse werkzaamheden is. Maar ook dat het aan alle leidinggevers is om ook op het hierbij behorende gedrag te sturen in de praktijk

- o er in de verticale verantwoordingslijnen minder sterk geleund wordt op één functionaris.

- Over het algemeen was het lastig om inzicht te krijgen in de benodigde documenten. Van de ene kant is dit begrijpelijk omdat het over een gevoelig onderwerp gaat, waar soms geheimhouding van toepassing is. Maar van de andere kant sluit dit ook aan bij het beeld van het algemeen bestuur dat het lastig is om goed inzicht te krijgen in de risico's die het hoogheemraadschap loopt, en hoe deze gemitigeerd zijn. De bereidheid van de ambtelijke organisatie om te communiceren over dit onderwerp heeft direct effect op het vertrouwen van het algemeen bestuur. Het is dus belangrijk dat er een juiste vorm van transparantie is om te zorgen dat het algemeen bestuur zich betrokken voelt bij dit onderwerp en daarmee ook het vertrouwen heeft in de borging hiervan.

## 4. In hoeverre is het algemeen bestuur in staat om te beoordelen of de digitale veiligheid binnen het Hoogheemraadschap De Stichtse Rijnlanden voldoende is geborgd om de primaire taakstelling en verantwoordelijkheden te verzekeren?

- Door gebrek aan kennis van het algemeen bestuur op dit onderwerp vindt men het lastig om goed te kunnen oordelen hierover. Vergelijkend onderzoek met bijvoorbeeld andere waterschappen zou hen daarbij kunnen helpen. Het zou daarom handig zijn als het Dagelijks Bestuur dit soort onderzoeken (bijvoorbeeld vanuit het waterschapshuis) kan delen met het algemeen bestuur. Hierbij is het wel belangrijk om te melden dat alhoewel dit leidt tot inzicht, niet per definitie tot het goede inzicht hoeft te leiden; immers het hoogheemraadschap kan op sommige gebieden een andere risicoprofiel hebben waardoor men eigenlijk tot andere maatregelen zou moeten komen dan collega waterschappen. Bovendien zegt de stand van zaken bij andere waterschappen niet veel over of je voldoet aan alle wettelijke eisen,

bijvoorbeeld in het geval dat alle waterschappen hier aan voldoen. Met andere woorden; vergelijkend onderzoek leidt tot inzicht, maar niet tot het volledige beeld.

- Naast rapportage zien we het gebrek aan kennis over het onderwerp en eventuele bewustwording van die eerder genoemde risico's op bestuurlijk niveau. Voor de toenemende urgentie van een goede informatiebeveiliging, zowel maatschappelijk als voor de organisatie zelf, zien we het als essentieel dat deze basiskennis ook op bestuurlijk niveau wordt opgebouwd. Denk daarbij aan kennis over de beleidskaders en de ontwikkelingen op landelijk en regionaal niveau, zodat bijvoorbeeld, als het Nationaal Cyber Security Centrum een bepaalde ontwikkeling rapporteert, het algemeen bestuur in staat is om dit te vertalen naar de situatie waar zij verantwoordelijk voor is

---

#### **Aanleiding:**

---

Met de toegenomen digitalisering van onze samenleving vormen cybercrime en andere inbreuken op de informatieveiligheid steeds serieuzere bedreigingen voor publieke organisaties, burgers en bedrijven. Een reeks kleinere en grote incidenten in het recente verleden hebben Nederland en de wereld bewuster gemaakt van de grote gevolgen die dergelijke incidenten kunnen hebben. Het wordt steeds duidelijker dat geen enkel individu of organisatie zich immuun kan wanen voor digitale dreigingen.

Ook voor HDSR groeit die afhankelijkheid van informatie en digitalisering. Enerzijds kent het Hoogheemraadschap de operatie, de bediening van gemalen en RWZI's, dat ondersteund wordt door meet- en bedieningssystemen. Anderzijds is HDSR een ambtelijke organisatie, met circa 400 medewerkers en benodigde werkplekken, applicaties en administratieve informatiestromen (inclusief eventuele privacy gevoelige informatie). Beide functies zijn van bedrijfskritisch en zelfs maatschappelijk belang, waarbij de vatbaarheid voor digitale dreiging in toenemende mate een rol speelt op zowel operationeel als bestuurlijk niveau.

Het is voor het Algemeen Bestuur belangrijk om zicht te hebben op de wijze waarop HDSR omgaat met informatieveiligheid en de risico's die zij loopt.

---

#### **Doel van dit voorstel:**

---

Kennisnemen van de uitkomsten van het onderzoek van de rekenkamercommissie met betrekking tot borging en verantwoording ten aanzien van digitale veiligheid.

De rekenkamercommissie wil het algemeen bestuur met dit onderzoek inzicht geven in de mate waarin het hoogheemraadschap en met name het algemeen bestuur inzicht heeft in beleid en rapportage omtrent informatieveiligheid en de risico's die HDSR ten aanzien van dit onderwerp loopt.

---

#### **Participatie:**

---

Het CDH heeft een reactie gegeven op het rapport. Deze is bijgevoegd.

---

#### **Nawoord van de rekenkamercommissie:**

---

De Rekenkamercommissie zegt het College van Dijkgraaf en Hoogheemraden dank voor haar reactie d.d. 20 maart 2018. De reactie is integraal aan dit bestuursvoorstel bijgevoegd. De Rekenkamercommissie heeft met belangstelling kennis genomen van de reactie op de conclusies van het rapport.

Ten aanzien van de reactie van het bestuur op de aanbevelingen van de commissie neemt de commissie er met instemming nota van dat het College de behoefte bij het

algemeen bestuur onderkent aan meer bagage, meer betrokkenheid en meer informatierijkheid.

De Rekenkamercommissie is verheugd dat het College in het rapport bevestiging vindt van het gevoerde beleid maar ook aanleiding ziet om met het Algemeen Bestuur te onderzoeken op welke wijze het Algemeen Bestuur op het onderwerp van digitale veiligheid nauwer kan worden betrokken en tot meer bevredigend inzicht kan komen.

---

**Communicatie:**

---

Het rkc-rapport wordt op de website van het Hoogheemraadschap De Stichtse Rijnlanden geplaatst.

---

**Financiën:**

---

n.v.t.

---

Houten, 30 maart 2018



Wijnand van de Giessen  
Voorzitter rkc HDSR



Koos Kappert  
Secretaris rkc HDSR

---

**Meegezonden bijlagen bij dit bestuursvoorstel:**

---

- 1.RKC HDSR Rapport Quicksan Digitale Veiligheid 20-2-2018
  - 2.Bestuurlijke reactie CDH (kenmerk 1368299)
-

# Bestuursbesluit



Voorstelnummer: 2018-003

Het Algemeen Bestuur van het Hoogheemraadschap De Stichtse Rijnlanden heeft het bestuursvoorstel d.d. 30 maart 2018 nr. 2018-003 gelezen en besluit:

- 1) Kennis te nemen van de resultaten van het onderzoek van de rekenkamercommissie met betrekking tot borging en verantwoording ten aanzien van digitale veiligheid.
- 2) In te stemmen met de aanbevelingen van het rapport, zoals genoemd in het bestuursvoorstel 2018-003

Dit is besloten in de openbare vergadering van het Algemeen Bestuur op 16 mei 2018.

Het Algemeen Bestuur van het Hoogheemraadschap De Stichtse Rijnlanden,

P.J.M. Poelmann  
Voorzitter

J. Goedhart  
Secretaris