waterschap Hollandse Delta

Datum: 26 oktober 2026
Status: Definitief

Bestuurlijke nota onderzoek Cybersecurity

Rekenkamer waterschap Hollandse Delta

Verantwoording

Waterschap	waterschap Hollandse Delta Handelsweg 100 2988 DC Ridderkerk Postbus 4103 2980 GC Ridderkerk t 088 974 33 00 i www.wshd.nl	
Afdeling	Rekenkamer waterschap Hollandse Delta	
Auteur/coördinatie	B. Nootenboom W. van Riel A. Hengeveld	b.nootenboom@wshd.nl w.vanriel@wshd.nl a.hengeveld@wshd.nl
Versie	26 oktober 2026 Definitief	

Inhoudsopgave

Verantwoording **2**

1 Inleiding **4**

2 Cybersecurity bij WSHD **5**

3 Bevindingen **6**

4 Conclusies en aanbevelingen **8**
4.1 Conclusies 8
4.2 Aanbevelingen 9

1 Inleiding

De Rekenkamer van waterschap Hollandse Delta onderzocht de mate waarin Waterschap Hollandse Delta zicht heeft op digitale risico's van de assets, hoe deze risico's worden beheerst en welke informatie hierover beschikbaar is voor de leden van de Verenigde Vergadering.

De centrale vraag is: *Hoe beheerst Waterschap Hollandse Delta de risico's op het gebied van cybersecurity van de assets (gemalen, sluizen e.d.), en hoe worden deze risico's inzichtelijk gemaakt voor de Verenigde Vergadering?*

Deze hoofdvraag is verdeeld in de volgende onderzoeksvragen:

- Wat is het beleid en strategie omtrent cybersecurity bij de WSHD?
- Welke risico's als gevolg van digitalisering worden onderkend door het waterschap? Welke maatregelen (processen, systemen, protocollen) zijn getroffen om deze risico's te beheersen?
- Hoe worden de rapportages over beheersing van de cybersecurityrisico's extern gevalideerd?
- Welke rol spelen medewerkers in de buitendienst bij het beheersen van de risico's en worden ze voldoende uitgerust (materieel en middels instructie) om de risico's te beheersen?
- Hoe vindt monitoring en evaluatie van deze maatregelen plaats?
- Welke informatievoorziening ontvangen de leden van de Verenigde Vergadering over cybersecurityrisico's en de hierbij behorende beheersmaatregelen?

Deze onderzoeksvragen zijn beantwoord in de nota van bevindingen, die als bijlage is gevoegd bij deze bestuurlijke nota en die op ambtelijk niveau is geverifieerd tijdens het ambtelijk wederhoor.

Voor dit onderzoek geldt de volgende afbakening: dit onderzoek richt zich op de beheersing van digitale risico's over de informatieveiligheid voor bediening van de assets (zoals gemalen, sluizen e.d.) in de primaire processen (niet zijnde kantoorautomatisering). Het onderzoek is verkennend van aard en bevat geen diepgaande technische audit.

Deze bestuurlijke nota heeft twee functies. Zij blikt terug op de periode mei 2025 – februari 2026 en toetst wat de rekenkamer heeft aangetroffen aan een referentiekader dat is ontleend aan de Waterschapswet, de Baseline Informatiebeveiliging Overheid 2 (BIO2) en de NIS2-richtlijn. De BIO2 is mede door de Unie van Waterschappen vastgesteld en geldt daarmee ook voor WSHD.[1]

Daarnaast kijkt de rekenkamer vooruit. De Cyberbeveiligingswet, die de NIS2-richtlijn in Nederland implementeert, was gedurende die onderzoeksperiode niet van kracht; zij is op 15 augustus 2026 in werking getreden. De rekenkamer toetst daarom niet aan de materiële eisen van die wet, maar hanteert haar als voorbereidingsnorm: van WSHD mag redelijkerwijs worden verwacht dat het zich op de inwerkingtreding voorbereidt en dat die voorbereiding zichtbaar is.

De Rekenkamer heeft het onderzoek langs drie lijnen uitgevoerd. De rekenkamer heeft relevante documenten opgevraagd en bestudeerd. Een eerste analyse van deze stukken leidde tot een schriftelijke technische vragenronde. Aan de hand van de stukken en van de verstrekte schriftelijke antwoorden zijn interviews gehouden met de diverse sleutelpersonen (zowel ambtelijk als bestuurlijk) binnen en buiten het waterschap Hollandse Delta.

Een tweede bron van informatie waren interviews, zowel intern als extern. Het doel van de interviews met medewerkers is het nagaan hoe de beleidsvoornemens in de praktijk toegepast worden en hoe de geïnterviewden zich verhouden tot cybersecurity.

Een derde ingezette bron is een enquête. Ter voorbereiding op het gesprek met de klankbordgroep is gebruik gemaakt van een enquête onder VV-leden. De enquête is gebruikt om de betrokkenheid en informatiepositie van VV-leden te kunnen bepalen.

[1] De Cyberbeveiligingsregeling sector overheid, die de BIO2 en NEN-EN-ISO/IEC 27002:2022 aanwijst als invulling van de zorgplicht, geldt niet voor de waterschappen. Voor hen geldt de Cyberbeveiligingsregeling IenW, met de Inspectie Leefomgeving en Transport als toezichthouder in plaats van de Rijksinspectie Digitale Infrastructuur.

2 Cybersecurity bij WSHD

Digitale veiligheid wordt bij WSHD serieus genomen. De waterschappen in Nederland, waaronder WSHD, werken met onder meer het Computer Emergency Response Team Watermanagement (CERT), Rijkswaterstaat en het Nationaal Cyber Security Centrum aan sectorbrede analyses en dreigingen.

De wetgeving rond Cybersecurity is de laatste jaren aan aanscherpingen onderhevig. Het heeft een paar jaar geduurd totdat de aanvullende afspraken op het bestuursakkoord Water in 2018 over onder andere de kansen van de informatiesamenleving én over de risico's van digitale dreigingen op landelijk niveau omgezet zijn in concrete beheersingsmaatregelen voor WSHD. De Europese NIS2 richtlijn (2022) is voor Nederland geïmplementeerd via de Cyberbeveiligingswet.

Het Waterschapshuis speelt voor WSHD een centrale ondersteunende rol door kennisdeling, standaardisatie, vertaling van wetgeving, gezamenlijke cybersecurity-oplossingen, CERT-diensten en trainingen voor medewerkers, management en bestuurders (o.a. over NIS2). Aan de hand van een in samenwerking met het Waterschapshuis ontwikkelde methode brengt WSHD sinds eind 2025 per asset de risico's en de bijbehorende beheersmaatregelen in beeld. Dit traject loopt nog: in 2026 volgt een nulmeting waarmee de feitelijke stand van de maatregelen wordt vergeleken met de gewenste.

Beleidskeuzes en door de VV vastgelegde ambities op het gebied van digitale veiligheid (zoals het behalen van trede 3 van de Veiligheidsladder en volwassenheidsniveau 4 BIO/AVG) schetsen een stip op de horizon waar WSHD naartoe werkt. WSHD werkt aan versterking van registratie en monitoring.

De Veiligheidsladder en de BIO/AVG-volwassenheidsniveaus bieden instrumenten om veiligheidscultuur en volwassenheid te meten en te verbeteren, met als doel risicogestuurd, proactief en continu verbeterend te werken aan informatie- en cyberbeveiliging.

De organisatie is zich gedurende de onderzoeksperiode blijven doorontwikkelen. Waar de rekenkamer heeft kunnen vaststellen dat een tekortkoming inmiddels is weggenomen – zoals de herpositionering van de CISO naar de concernstaf – is dit in de nota van bevindingen vermeld.

3 Bevindingen

Aan de hand van een referentiekader en de beantwoording van de onderzoeksvragen zijn in de nota van Bevindingen 30 bevindingen opgenomen. Deze bevindingen leiden soms tot een conclusie, maar geven op zijn minst aanleiding om over het onderwerp Cybersecurity nadere gesprekken te voeren tussen de VV en D&H. Het gaat dan met name over de governance: waar ligt de grens tussen de verantwoordelijkheid van VV, D&H en de organisatie? Die vraag is met de Cyberbeveiligingswet onontkoombaar geworden: de wet vereist dat de rolverdeling belegd én aantoonbaar is.

1. Risicoanalyse en -beheersingsmaatregelen

Voor alle fysieke assets binnen de afvalwaterketen en het watersysteem wordt sinds eind 2025 gewerkt met de inventarisatie van cyberrisico's en het in beeld brengen van corresponderende beheersmaatregelen.

2. Beleidsvaststelling en positie VV

De rekenkamer ziet op grond van de Waterschapswet het vaststellen van beleid (dus ook het strategisch informatiebeveiligingsbeleid) als een verantwoordelijkheid van de VV. De Cyberbeveiligingswet legt de verantwoordelijkheid voor het informatiebeveiligingsbeleid bij het dagelijks bestuur, in dit geval dus D&H. Beide sporen laten zich verenigen, de VV stelt kaders en controleert, D&H stelt het beleid vast en legt verantwoording af, maar dan moet die verdeling wel ergens zijn vastgelegd. Dat is nu niet het geval. De rekenkamer heeft vastgesteld dat de VV het informatiebeveiligingsbeleid niet heeft vastgesteld en dat in het governanceplan informatiebeveiliging de VV helemaal niet wordt genoemd.

De VV heeft slechts één besluit genomen dat door D&H en ambtelijke organisatie als kader voor Cybersecurity wordt gehanteerd. In 2022 is door de VV besloten dat Trede 3 van de NEN-veiligheidsladder eind 2023 en trede 4 AVG/BIO in 2024 moet zijn bereikt.

De VV wordt niet actief geïnformeerd over risico's of te nemen maatregelen als gevolg van cyberdreiging. Rapportages van de CISO en FG komen niet bij de VV terecht.

In de enquête geven VV leden aan de nadrukkelijke wens te hebben om meer betrokken te worden bij het onderwerp cybersecurity. Er is geen initiatief genomen (niet door de VV, noch door D&H) om het gesprek te voeren of en zo ja welke rol de VV wenst te hebben op het terrein van cybersecurity.

3. Positie D&H

D&H wordt in een aantal gevallen niet actief in positie gebracht om bij te sturen. Zo zijn niet alle externe auditrapporten gedeeld met de heemraad of D&H en heeft het in 2025 8 maanden geduurd voordat de CISO/FG rapportage werd besproken in D&H. Actiepunten uit de CISO/FG rapportage zijn opgenomen in de verbeteragenda. Deze halfjaarlijkse verbeteragenda die aan D&H wordt aangeboden bevat veel actiepunten en deadlines. Niet alle actiepunten uit (externe) audits zijn opgenomen in de verbeteragenda. Daarnaast kan vanwege de hoeveelheid actiepunten niet alles meteen opgevolgd worden. Opgenomen actiepunten zijn voorzien van een planningsdatum.

Onvoldoende opvolging als gevolg van bovenstaande bevindingen duidt op een tekortkoming in zowel de sturing door de directie als het toezicht door D&H. Daardoor is niet zichtbaar welke actiepunten open staan en welke risico's daarmee blijven bestaan. Zowel de directie als D&H mist hierdoor het overzicht dat nodig is om te sturen. De Cyberbeveiligingswet vereist dit echter wel als aantoonbaar bewijs van toezicht.

Met de inwerkingtreding van de Cyberbeveiligingswet wordt bestuurlijke betrokkenheid bij informatieveiligheid een expliciete en aantoonbare verplichting. De wet legt de eindverantwoordelijkheid bij het dagelijks bestuur en stelt eisen aan kennis, toezicht en documentatie daarvan.

4. Tot slot

Gedurende de looptijd van het onderzoek heeft de rekenkamer een toenemende urgentie binnen de ambtelijke organisatie waargenomen waar Cybersecurity als thema binnen WSHD werd geagendeerd. Er is in 2024 een cybersecurityteam gestart, er is met de andere waterschappen een gedeelde werkwijze opgezet, de CISO is onafhankelijker gepositioneerd en de risico's per asset worden in kaart gebracht. Die beweging is de basis waarop deze nota voortbouwt: niet de vraag wat er is misgegaan, maar de vraag wat er in 2026 en verder nodig is om het bereikte te borgen.

4 Conclusies en aanbevelingen

Het doel van het onderzoek is om te bepalen of het Waterschap Hollandse Delta zicht heeft op digitale risico's van de assets, hoe deze risico's worden beheerst en welke informatie hierover beschikbaar is voor de leden van de Verenigde Vergadering.

4.1 Conclusies

1. Risicoanalyse en -beheersing van cybersecurity is binnen WSHD geborgd en er wordt continu gewerkt aan verbetering van informatie- en cyberbeveiliging.
   - De risicoanalyse en -beheersing van cybersecurity is bij WSHD in opzet ingericht en in ontwikkeling.
   - De organisatie heeft aantoonbaar stappen gezet: een gezamenlijke werkwijze met het Waterschapshuis, een inventarisatie van cyberrisico's per asset, technische monitoring via de regiekamer, trainingen voor medewerkers en een onafhankelijker positie voor de CISO.

2. De VV vervult haar kaderstellende en controlerende rol op dit terrein nog niet, en is daartoe ook niet in staat gesteld
   - Er is over cybersecurity geen debat gevoerd, geen initiatief genomen, geen vragen gesteld en er zijn geen moties ingediend.
   - De VV heeft een kader gesteld over de na te streven trede op de NEN-veiligheidsladder en de mate van AVG/BIO volwassenheid. De VV is ad hoc geïnformeerd over de voortgang van implementatie van trede 3 NEN-veiligheidsladder en AVG/BIO volwassenheid. Verschuiving van de deadline door D&H heeft niet geleid tot een debat of vragen.
   - Vaststelling van strategische beleidsstukken over cybersecurity gebeurt niet door de VV en er wordt niet gerapporteerd over cyberrisico's en beheersing.
   - De VV wordt op onregelmatige basis informeel bijgepraat over cybersecurity.

3. D&H wordt onvoldoende in staat gesteld te sturen op de voortgang van aanbevelingen uit rapportages en externe audits.
   - Niet alle externe auditrapporten bereiken het college, de CISO/FG-jaarrapportage over 2024 werd pas acht maanden na verschijnen in D&H besproken en een actueel overzicht van open actiepunten ontbreekt. Dat is deels een kwestie van aanlevering door de organisatie en deels van doorpakken door D&H zelf. Zolang dit beeld ontbreekt, kan D&H zijn toezicht ook niet aantoonbaar maken.

4.2 Aanbevelingen

De conclusies in voorgaande paragraaf leiden tot de volgende aanbevelingen.

Aanbeveling 1. **Geef D&H de opdracht een bestuurlijk gesprek voor te bereiden over de rol van de VV bij cybersecurity.**

Uit de enquête onder VV-leden en het gesprek met de klankbordgroep blijkt dat VV leden het onderwerp cybersecurity een aangelegen onderwerp vinden. Door te spreken over de rol van de VV komt er duidelijkheid over de governance. (NB. Deze rol dient vervolgens ook verwerkt te worden in de beschrijving van de governanceplan).

Daarnaast dient het gesprek ook om afspraken te maken over de manier waarop en in welke frequentie de VV geïnformeerd wenst te worden over cybersecurity risico's en bijbehorende beheersmaatregelen. De informatiebehoefte van de VV gaat verder dan af en toe een mededeling over de stap op de veiligheidsladder of het niveau van volwassenheid AVG/BIO.

In dit gesprek kan ook de paradox aan de orde komen hoe het komt dat er kennelijk een grote behoefte bij de VV bestaat om meer betrokken te worden bij het onderwerp cybersecurity, maar dat er geringe belangstelling vanuit de VV is op het moment dat er een bijeenkomst wordt georganiseerd over dit onderwerp.

Aanbeveling 2. Geef D&H de opdracht een monitoringsprogramma op te zetten om actueel zicht te houden op de opvolging van aanbevelingen van (externe) audits.

De wereldwijde ontwikkeling bij cybersecuritydreigingen gaat snel. De halfjaarlijkse update van de verbeteragenda biedt onvoldoende (bij)sturingsmogelijkheden voor D&H om goed in te kunnen spelen op de actualiteit. Als gevolg hiervan kan de VV ook onvoldoende worden geïnformeerd over de voortgang van de opvolging van de aanbevelingen van (externe) audits.

Een dergelijk programma hoeft niet zwaar te zijn. Een doorlopend overzicht van openstaande actiepunten uit interne en externe audits, met eigenaar, deadline en status, volstaat – mits het actueel is en periodiek in D&H wordt besproken. Dit kan een doorontwikkeling zijn van de huidige verbeteragenda, die actueel inzicht geeft in de opvolging van de verbeteringen. Datzelfde overzicht levert de aantoonbaarheid van toezicht die de Cyberbeveiligingswet vraagt, en vormt de basis voor de rapportage aan de VV.

Aanbeveling 3. Geef D&H de opdracht het beleidskader informatieveiligheid aan de VV voor te leggen en daarin de rol van elk orgaan te beschrijven.

Het Informatiebeveiliging Governance Plan bestaat sinds januari 2025. De daarin aangekondigde KPI's zijn nog niet uitgewerkt. Het Strategisch Informatiebeveiligingsbeleid is niet aan de VV voorgelegd. In beide stukken ontbreekt de VV als actor.

De Cyberbeveiligingswet en de BIO2 vragen om een aantoonbaar managementsysteem en om bestuurlijke betrokkenheid die gedocumenteerd is; het jaar 2026 is daarvoor het natuurlijke moment. De uitkomst van het gesprek uit aanbeveling 1 kan hierin worden verwerkt.