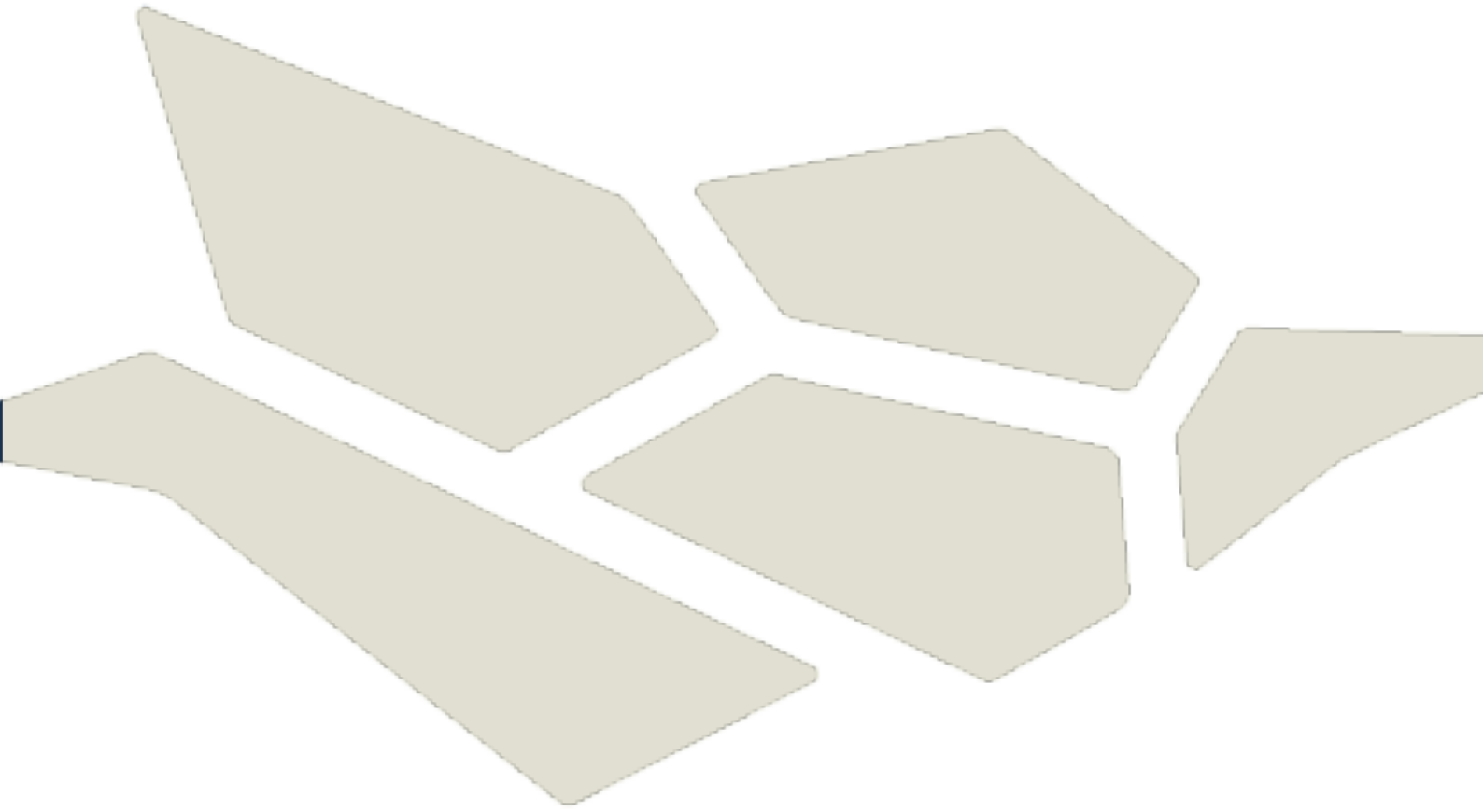
waterschap Hollandse Delta

Datum: 17 juli 2026
Status: Definitief

Nota van Bevindingen Onderzoek Cybersecurity

Rekenkamer waterschap Hollandse Delta



Nota van Bevindingen Onderzoek Cybersecurity 17 juli 2026

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	17 juli 2026 Definitief	

Begrippenlijst

Afkorting	Verklaring
AVG (GDPR)	Algemene Verordening Gegevensbescherming (General Data Protection Regulation). Europese privacywet
BIO	Baseline Informatiebeveilging Overheid
BIO2	Baseline Informatiebeveiliging Overheid 2 is het verplichte normenkader voor informatiebeveiliging binnen de gehele Nederlandse overheid geldend vanaf september 2025.
CER-richtlijn	Critical Entities Resilience Directive
CERT WM	Computer Emergency Response Team Watermanagement
CBW	Cyberbeveiligingswet
IPO	Interprovinciaal Overleg
NCSC	Het Nationaal Cyber Security Centrum is een onderdeel van het ministerie van Justitie en Veiligheid en valt onder de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)
NEN-ISO/IEC 27001	Wereldwijd erkende norm op het gebied van informatiebeveiliging
NEN-ISO/IEC 27002	Informatiebeveiliging, Cybersecurity en Bescherming van Privacy – Praktische richtlijnen voor informatiebeveiligingsmaatregelen
NIS2	Network and Information Security Directive 2. Het is de tweede versie van de Europese NIS-richtlijn, die de cyberweerbaarheid van vitale en belangrijke sectoren in de EU moet verbeteren. De richtlijn is omgezet in Nederland via de Wet beveiliging netwerk- en informatiesystemen 2 – (Wbni2: de zogenoemde 'Cybersecuritywet').
UvW	Unie van Waterschappen
SIEM	Security Information and Event Management
SOC-RWS	Security Operation Center van Rijkswaterstaat
STOWA	Stichting Toegepast Onderzoek Waterbeheer
TA	Technische Automatisering
Vewin	Verenging van waterbedrijven in Nederland
VNG	Vereniging van Nederlandse Gemeenten
Wbni	Wet Beveiliging Netwerk- en Informatiesystemen
Wwke	Wet weerbaarheid kritieke entiteiten

Inhoudsopgave

Verantwoording **2**

Begrippenlijst **3**

1 Inleiding **5**

2 Doel en onderzoeksaanpak **6**
2.1 Doel en onderzoeksvragen 6
2.2 Aanpak 6
2.3 Afbakening 6
2.4 Referentiekader 7

3 Context en referentiekader **8**
3.1.1 Verenigde Vergadering 9
3.1.2 College van Dijkgraaf en Heemraden 10
3.1.3 Directie en management 11
3.1.4 Chief Information Security Officer (CISO) 12

4 Bevindingen en toetsing aan referentiekader **13**
4.1 Beleid, strategie en governance 13
4.2 Governance bij WSHD 14
4.3 Risicobeheersing, maatregelen en uitvoering 18
4.4 Monitoring, evaluatie en externe validatie 21
4.4.1 Monitoring maatregelen 21
4.4.2 Audit 22
4.5 Bestuurlijke informatievoorziening en rol van de VV 25

Referenties **28**

Bijlage 1. Geïnterviewde functionarissen **29**

Bijlage 2. Enquête voor klankbordgroep **30**

Bijlage 3: Veiligheidsladder **32**

1 Inleiding

Bijna dagelijks worden artikelen gepubliceerd waarin de digitale dreiging op publieke organisaties wordt geduid. De Rijksoverheid richt zich middels een publiekscampagne op vergroting van de weerbaarheid van de gehele samenleving. Regelmatig verschijnen berichten over cyberaanvallen op publieke instellingen of overheden door hackergroepen of statelijke actoren zoals China of Rusland. De digitale dreiging richting publieke organisaties neemt toe. Voor waterschappen betekent dit dat vitale processen, zoals waterveiligheid, waterzuivering en peilbeheer, in toenemende mate afhankelijk zijn van goed beveiligde digitale systemen.

Daarnaast liet de stroomuitval bij een waterzuiveringsinstallatie in Haps op 25 november 2025 een beeld zien van beginnende ontwrichting van de maatschappij als de assets niet meer ingezet kunnen worden. Deze stroomuitval was weliswaar niet het gevolg van een cyberaanval, maar gaf wel beeld van verstoring van de samenleving.

Het bestuursakkoord water uit 2011 (waarin door de Unie van Waterschappen, Interprovinciaal Overleg, Vereniging van waterbedrijven in Nederland, Ministerie van Infrastructuur en Waterstaat en Vereniging van Nederlandse Gemeenten afspraken werden gemaakt om de doelmatigheid van het waterbeheer te vergroten) kreeg in 2018 aanvullende afspraken over onder andere de kansen van de informatiesamenleving én over de risico's van digitale dreigingen.

De afspraak werd gemaakt om deze aanvullende afspraken op het Bestuursakkoord Water uit te voeren. De stuurgroep Water is verantwoordelijk voor de uitvoering van deze afspraken en bewaakt de voortgang[1].

Nu, 7 jaar na het afsluiten van de aanvullende afspraken uit het Bestuursakkoord Water is het tijd om te beoordelen hoe het waterschap Hollandse Delta zicht heeft en omgaat met digitale risico's.

De rekenkamer wil in dit onderzoek inzicht krijgen in:

- De mate waarin Waterschap Hollandse Delta zicht heeft op digitale risico's van de assets
- Hoe deze risico's worden beheerst
- Welke informatie hierover beschikbaar is voor de leden van de Verenigde Vergadering

In deze nota van bevindingen heeft de Rekenkamer de bevindingen uit het onderzoek (hoofdstuk 4) getoetst aan normen in de vorm van het referentiekader (hoofdstuk 3). Het onderzoek heeft plaatsgevonden in de periode mei 2025 – februari 2026. Enkele bevindingen uit deze periode zijn na deze onderzoeksperiode opgelost.

[1] Unie van Waterschappen, *Aanvullende afspraken Bestuursakkoord Water* (2018), https://unievanwaterschappen.nl/wp-content/uploads/2021/11/Toekomstvisie-Bestuursakkoord-Water-2018.pdf.

2 Doel en onderzoeksaanpak

2.1 Doel en onderzoeksvragen

De digitale dreiging richting publieke organisaties neemt toe. Voor waterschappen betekent dit dat vitale processen, zoals waterveiligheid, waterzuivering en peilbeheer, in toenemende mate afhankelijk zijn van goed beveiligde digitale systemen.

Het doel van dit onderzoek is het verkrijgen van inzicht in de risicobeheersing van cybersecurity bij fysieke objecten van het waterschap, en de informatievoorziening daarover naar de VV.

De hoofdvraag van het onderzoek luidt:

> *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?*

Bovenstaande hoofdvraag is opgedeeld in de volgende deelvragen.

- 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?

2.2 Aanpak

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 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. De geïnterviewde functionarissen zijn opgesomd in bijlage 1.

Een derde ingezette aanpak 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.

2.3 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.

Als we kijken naar de term 'risicobeheersing' in het doel van het onderzoek, gaat dit verder dan enkel het identificeren van risico's en het beschrijven van maatregelen per risico. Een adequate risicobeheersing vloeit voort uit een gedegen beleidsvoorbereiding, uitvoering, controle en

evaluatie. In andere woorden, de governance. In de beantwoording van de onderzoeksvragen zal dit ook nadrukkelijk tot uiting komen.

2.4 Referentiekader

Het volgende hoofdstuk beschrijft een referentiekader dat wordt gebruikt bij het beoordelen van de bevindingen. Bij deze beoordeling is de volgende categorisering gebruikt.

- ✅ Voldoet aan de norm
- 🟡 Voldoet gedeeltelijk aan de norm
- ❌ Voldoet niet aan de norm

In deze nota van bevindingen heeft de Rekenkamer de bevindingen uit het onderzoek (hoofdstuk 4) getoetst aan normen in de vorm van het referentiekader (hoofdstuk 3). Omdat dit onderzoek deels een ex-ante karakter heeft, richt de toetsing zich niet op wat al bereikt is, maar op de vraag of toekomstige voorwaarden reeds aanwezig zijn om de beoogde doelen te kunnen realiseren. Bij ex-ante onderzoek fungeert de toetsing als een vroegtijdige signalering.

3 Context en referentiekader

Cybersecurity is het geheel aan maatregelen om risico's met betrekking tot informatieveiligheid tot een aanvaardbaar niveau te reduceren. De maatregelen kunnen zijn gericht op het voorkomen van cyberincidenten en - wanneer cyberincidenten zich hebben voorgedaan - deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau is, is de uitkomst van een risicoafweging.

Volgens de Waterschapswet berusten in principe alle bevoegdheden tot regeling en bestuur bij het algemeen bestuur van het waterschap. Het algemeen bestuur stelt beleid en regels vast, bepaalt de belasting en controleert de uitvoering door het dagelijks bestuur. Het dagelijks bestuur voert het beleid uit, verzorgt de dagelijkse gang van zaken en legt hierover verantwoording af aan het algemeen bestuur, dat recht heeft op alle benodigde informatie.

Voor een beoordeling van de governance van cybersecurity bij WSHD, hanteert de rekenkamer een referentiekader dat is gebaseerd op de verantwoordelijkheden die voortvloeien uit de Waterschapswet, de (in 2026 in werking tredende) Cyberbeveiligingswet (CBW), de Baseline Informatiebeveiliging Overheid 2 (BIO2)[2] en de NIS2-richtlijn[5]. Dit referentiekader beschrijft per actor de minimale verwachtingen ten aanzien van sturing, uitvoering, toezicht en verantwoording op het gebied van cybersecurity.

Het referentiekader is gestructureerd langs vier actoren/functies die elk een eigen en onderscheidende rol vervullen. Het is van belang dat deze rollen niet alleen formeel zijn belegd, maar ook daadwerkelijk worden uitgevoerd en aantoonbaar gemaakt. Juist de Cyberbeveiligingswet vereist dat bestuurlijke betrokkenheid 'evidence based' is: het toezicht moet zichtbaar gedocumenteerd zijn zodat extern toezicht zich daarop kan baseren.

Dit referentiekader is ontleend aan de volgende wet- en regelgeving en normenkaders:

- Waterschapswet[3]. Deze bepaalt de bevoegdheidsverdeling tussen VV (algemeen bestuur), D&H (dagelijks bestuur) en de ambtelijke organisatie (art. 10, 56, 77, 83, 95, 108).
- Cyberbeveiligingswet[4] (CBW). Deze maakt cyberbeveiliging een expliciete bestuurlijke verantwoordelijkheid, stelt eisen aan zorgplicht (art. 21), bestuurlijke verantwoordelijkheid en verplichte opleidingen (art. 24) en meldplicht bij incidenten (art. 25). Let op: de CBW was bij het opstellen van dit rapport (februari 2026) nog niet in werking getreden. De verwachte inwerkingtreding is Q2 2026. De rekenkamer baseert zich op dit moment op het wetsvoorstel zoals ingediend bij de Tweede Kamer op 4 juni 2025. Desondanks is deze wet wel opgenomen in het referentiekader, omdat er redelijkerwijs verwacht mag worden dat WSHD zich hierop voorbereidt.
- NIS2-richtlijn (EU 2022/2555) [5]. De Europese richtlijn die governance-verantwoordelijkheden van bestuursorganen regelt (art. 20) en eisen stelt aan cyberrisicobeheermaatregelen (art. 21) en incidentmelding (art. 23). In Nederland is de NIS2-richtlijn geïmplementeerd via de CBW.
- Baseline Informatiebeveiliging Overheid versie 2 (BIO2) [2]. Dit verplichte normenkader voor alle overheidslagen geldt vanaf september 2025. Deze is gebaseerd op ISO/IEC 27001:2023 en ISO/IEC 27002:2022 en schrijft een risicogerichte aanpak, een Information Security Management System (ISMS) en aantoonbare verantwoording voor.
- Cybersecurity Implementatierichtlijn Objecten versie 3.4 (CSIR 3.4) [6]. Dit is specifieke richtlijn voor beveiliging van procesautomatisering en operationele technologie bij

[2] Rijksoverheid e.a., *BASELINE INFORMATIEBEVEILIGING OVERHEID 2 - BIO 2* (2026).
[3] Waterschapswet (2024), https://wetten.overheid.nl/BWBR0005108/2026-01-01.
[4] Wet weerbaarheid kritieke entiteiten, Staatsblad 2026, 188 (2026), https://zoek.officielebekendmakingen.nl/stb-2026-188.html.
[5] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2), EUR-lex 80 (2022), http://data.europa.eu/eli/dir/2022/2555/oj.
[6] Rijkswaterstaat en Het Waterschapshuis, *Cybersecurity Implementatierichtlijn Objecten*, versie 3.4 (2021), https://cuatro.sim-cdn.nl/certwm/uploads/csir-3.4-definitief-concept-20210914.pdf?cb=eKtH4fdi.

waterschappen. Deze combineert BIO en IEC 62443 en is van toepassing op assets zoals gemalen, sluizen en rwzi's.
- ISO/IEC 27001 en 27002. Dit zijn internationale normen voor informatiebeveiliging en beheersmaatregelen. Deze vormen de basis voor de BIO2.
- Critical Entities Resilience Directive (CER-richtlijn)[7]. Om de weerbaarheid van Europese lidstaten te versterken heeft de Europese Unie eind 2022 de CER-richtlijn aangenomen. Het doel daarvan is om onze essentiële diensten in Europa zo goed mogelijk te beschermen tegen allerlei soorten dreigingen, zoals de gevolgen van (terroristische) misdrijven, sabotage en natuurrampen. In Nederland is de CER-richtlijn geïmplementeerd in de Wet weerbaarheid kritieke entiteiten (Wwke) [8].

Binnen de watersector vormen cyberdreigingen een reëel risico voor vitale processen zoals waterkeringen, drinkwater, zuivering en waterketens. Uitval of verstoring kan grote gevolgen hebben voor volksgezondheid, veiligheid en economie. Daarom werken waterschappen samen via onder meer CERT Watermanagement, Rijkswaterstaat, het NCSC en sectorbrede analyses. De Vaarkaart Digitale Transformatie uit 2024 kan door waterschappen worden gebruikt om binnen het bestuur, het managementteam en/of binnen verschillende afdelingen het gesprek over de digitale transformatie te voeren.

Het Waterschapshuis speelt 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).

Beleidskeuzes en ambities (zoals het behalen van trede 3 van de Veiligheidsladder en volwassenheidsniveau 4 BIO/AVG) schetsen een stip op de horizon. WSHD werkt aan versterking van registratie en monitoring via onder meer een SIEM/SOC, een Incident Response Plan, en een risicogerichte aanpak per asset volgens de CISR-richtlijn, met nulmetingen en meerjarenprogrammering.

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 werken aan informatie- en cyberbeveiliging.

3.1.1 Verenigde Vergadering

De positie van de VV, het algemeen bestuur, is die van het hoogste democratisch orgaan van het waterschap.

Verantwoordelijkheid	Toelichting	Wettelijke grondslag
Beleid vaststellen	De VV stelt het beleid vast, of delegeert dit expliciet aan D&H met behoud van controlebevoegdheid.	Waterschapswet art. 56, 77; CBW art. 24
Zorgen voor middelen	De VV stelt via de begroting middelen beschikbaar voor de uitvoering van het beleid.	Waterschapswet art. 101
Controle op uitvoering door D&H	De VV controleert of het D&H de vastgestelde doelen heeft behaald	Waterschapswet art. 89
Informatiepositie organiseren	De VV maakt haar controlerende rol kenbaar en organiseert haar eigen informatiepositie	Reglement van Orde VV WSHD 2025 Hfst. V

Artikel 56 Waterschapswet stelt dat het waterschapsbestuur bevoegd is tot 'regeling en bestuur'. Deze bevoegdheid berust volgens artikel 77 bij het algemeen bestuur voor zover deze niet bij of

[7] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing, Legislation No. 32022L2557, EUR-Lex (2022), http://data.europa.eu/eli/dir/2022/2557/oj.
[8] Wet weerbaarheid kritieke entiteiten.

krachtens reglement dan wel bij wet of algemene maatregel van bestuur is toegekend aan het dagelijks bestuur of aan de voorzitter.

In zijn algemeenheid betekent dit dat het algemeen bestuur het beleid vaststelt tenzij dit bij een ander orgaan is belegd.

Voor dit onderzoek betekent dat:
VV1. De VV is aantoonbaar betrokken bij het vaststellen van strategisch cybersecuritybeleid.

VV2. De verantwoordelijkheidsverdeling tussen VV en D&H is vastgelegd.

VV3. De VV stelt budget ter beschikking voor het uitvoeren van het cybersecuritybeleid

De controlerende rol van de VV is in de Waterschapswet niet als zodanig benoemd, maar volgt indirect uit de structuur van de wet. De Waterschapswet spreekt over het afleggen van verantwoording en het vragen om inlichtingen door de leden van het algemeen bestuur.

VV4. De VV controleert op uitvoering van cybersecuritybeleid. Dit omvat minimaal bespreking van de CISO/FG-jaarrapportage, inzicht in externe audits en toetsing van de voortgang op de veiligheidsladder.

De instrumenten die de VV kan gebruiken bij haar controlerende taak, zijn geregeld in hoofdstuk V van het Reglement van Orde VV WSHD 2025 [9], art. 36 t/m 47: (sub-)amendementen, splitsing in onderdelen, moties, ordevoorstel, initiatiefvoorstellen, technische vragen, politiek bestuurlijke vragen, interpellatie, bespreeknotitie, rondvraag, mededeling en ambtelijke bijstand.

VV5. De VV zet bestuurlijke instrumenten in ter versterking van haar informatiepositie

3.1.2 College van Dijkgraaf en Heemraden

De positie van het D&H, het dagelijks bestuur, is die van het dragen van eindverantwoordelijkheid van de dagelijkse gang van zaken.

Verantwoordelijkheid	Toelichting	Wettelijke grondslag
Beleid voorbereiden en vaststellen	D&H bereidt het cybersecuritybeleid voor en stelt het vast.	Waterschapswet art. 84 lid 2; CBW art. 24 lid 1 en 12e
Eindverantwoordelijkheid	D&H is op grond van de CBW eindverantwoordelijk voor de implementatie van passende en evenredige technische, operationele en organisatorische maatregelen. D&H keurt maatregelen goed, houdt toezicht op de effectiviteit en beschikt aantoonbaar over voldoende kennis via verplichte opleidingen.	CBW art. 24 lid 1, 2 en 12e; BIO2 art. 12.1
Verantwoording aan de VV	D&H legt verantwoording af aan de VV over het gevoerde cybersecuritybeleid.	Waterschapswet art. 89 lid 1
Evaluatie en verbetering	Het informatiebeveiligingsbeleid wordt minimaal jaarlijks en in aansluiting bij de P&C-cyclus en externe ontwikkelingen beoordeeld en zo nodig bijgesteld. Evaluatie vindt o.a. plaats via audits.	BIO2, maatregel 5.01.02, 5.20.04, 5.35.02, 5.36.01
Verplichte opleiding voor bestuurders	Opleidingsverplichting, aantoonbare training op het gebied van cybersecurity	CBW art. 24, NIS2 art 20.2

[9] Waterschap Hollandse Delta, *Reglement van Orde VV WSHD 2025* (2025), https://lokaleregelgeving.overheid.nl/CVDR745840/1.

Volgens de Waterschapswet is in beginsel het algemeen bestuur het bevoegd orgaan voor het vaststellen van beleid. De Cyberbeveiligingswet legt echter de verantwoordelijkheid voor het informatiebeveiligingsbeleid bij het dagelijks bestuur.

Voor dit onderzoek betekent dat:

DH1. D&H bereidt het cybersecuritybeleid voor en stelt het vast.

DH2. D&H is aantoonbaar eindverantwoordelijk, neemt actief en tijdig kennis van rapportages en auditbevindingen, en legt hierover gestructureerd en volledig verantwoording af aan de VV waarbij de rapportages zijn afgestemd op de informatiewensen van de leden van de VV.

DH3. D&H draagt zorg voor een volledig en actueel beleidskader, inclusief het Governance Plan Informatiebeveiliging. De verantwoordelijkheidsverdeling tussen de VV en D&H is vastgelegd.

DH4. D&H legt verantwoording af o.a. via resultaten van externe audits, uitkomsten van CISO/FG-rapportages en opvolging van aanbevelingen daarvan.

DH5. D&H draagt zorg voor evaluatie en verbetering van beleid (jaarlijks, aansluitend op P&C cyclus, via audits)

DH6. De leden van D&H hebben aantoonbaar een opleiding gevolgd op het gebied van cybersecurity.

3.1.3 Directie en management

De positie van directie en management is die van verantwoordelijkheid dragen voor de uitvoering van het bestuurlijk vastgestelde beleid.

Verantwoordelijkheid	Toelichting	Norm
Beleid implementeren	De directie (in BIO2 wordt de actor 'lijnmanagement' gebruikt) vertaalt het vastgestelde cybersecuritybeleid naar concrete uitvoeringsmaatregelen, verantwoordelijkheden, capaciteit en draagt het beleid actief uit in de organisatie.	BIO2 art. 12 & maatregel 5.01.01
ISMS opstellen	De directie stelt een Information Security Management System (ISMS) op om informatiebeveiliging binnen de organisatie te borgen.	CBW art. 21; BIO2 (verplichting tot aantoonbaar ISMS)
Capaciteit organiseren	De directie organiseert de benodigde capaciteit (intern en extern) om het cybersecuritybeleid aantoonbaar uit te voeren, inclusief bezetting van de CISO-functie en budget voor trainingen en audits.	CBW art. 21 lid 2; NIS2 art. 21 lid 2g
Rapporteren aan D&H over uitvoering van risicobeheersing	Het lijnmanagement is verantwoordelijk voor het identificeren van dreigingen en risico's van informatiesystemen en stelt de bestuurder in staat om hun verantwoordelijkheid op het gebied van risicomanagement dat gericht is op het borgen van digitale weerbaarheid uit te voeren.	BIO2 art. 12; CBW art. 21

Voor dit onderzoek betekent dat:

D1. De directie heeft aantoonbaar het informatiebeveiligingsbeleid vertaald in concrete elementen voor de ambtelijke organisatie.

D2. De directie heeft een ISMS opgesteld om informatiebeveiliging aantoonbaar te borgen.

D3. De directie heeft capaciteit georganiseerd (intern/extern), inclusief bezetting en budget voor trainingen en audits

D4. De directie rapporteert over uitvoering van cybersecuritybeleid aan D&H.

3.1.4 Chief Information Security Officer (CISO)

De positie van de CISO is een onafhankelijke functionaris verantwoordelijk voor coördinatie, monitoring en advisering op het gebied van informatiebeveiliging.

Verantwoordelijkheid	Toelichting	Norm / richtlijn
Onafhankelijke positie	De CISO bekleedt een onafhankelijke positie. De onafhankelijkheid is formeel geborgd.	BIO2 art 12.3 & maatregel 5.02.01, 5.02.02
Rapporteren aan directie en D&H	De CISO rapporteert periodiek aan D&H over de staat van informatiebeveiliging, risico's en opvolging van aanbevelingen. De CISO geeft ook gevraagd en ongevraagd advies.	BIO2 art. 12.3

Voor dit onderzoek betekent dat:

C1. De CISO functioneert aantoonbaar onafhankelijk

C2. De CiSO rapporteert tijdig en volledig aan D&H over staat van informatiebeveiliging, risico's en opvolging aanbevelingen en adviseert gevraagd en ongevraagd aan de juiste gremia.

De expliciete rol van 'CISO' was in de vorige versie van BIO geen onderdeel van het toetsingskader.

4 Bevindingen en toetsing aan referentiekader

4.1 Beleid, strategie en governance

Deelvraag 1 Wat is het beleid en strategie omtrent cybersecurity bij WSHD

De basisafspraken over cybersecurity binnen de watersector vinden hun oorsprong in de Aanvullende afspraken Bestuursakkoord Water[1] (november 2018). Hierin is afgesproken dat het kwetsbare watersysteem wordt versterkt door de samenwerking tussen betrokken overheden op het gebied van digitale veiligheid in het watersysteem. Hierbij wordt aangesloten bij de landelijke aanpak van cybersecurity (o.a. Wet digitale overheid en Cybersecuritywet). Wettelijk wordt vereist dat WSHD technische en organisatorische maatregelen neemt om op risico's afgestemd beveiligingsniveau te waarborgen.

Het beleid en de strategie van WSHD liggen vast in het Strategisch Informatie Beveiligingsbeleid 2024-2026[10]. Dit beleidsplan geeft invulling aan de norm 5.1 "Aansturing door de directie van de informatiebeveiliging" van de Baseline Informatiebeveiliging Overheid (BIO). De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het besturen van de informatiebeveiliging
- Adequate bescherming van bedrijfsmiddelen
- Minimaliseren van de risico's van menselijk gedrag
- Voorkomen van ongeautoriseerde toegang
- Garanderen van correcte en veilige informatievoorzieningen
- Beheersen van de toegang tot informatiesystemen
- Waarborgen van veilige informatiesystemen
- Adequaat reageren op incidenten
- Beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers
- Waarborgen van de naleving van dit beleid.

Voor wat betreft procesautomatisering wordt rekening gehouden worden met de CER Richtlijn[7] en NIS2 [5], gericht op verbetering van de digitale en economische weerbaarheid van de Europese lidstaten.

Op het gebied van informatiebeveiliging vormt Het Waterschapshuis 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). Op strategisch gebied werken de waterschappen samen in het Digitaliserings Beraad. Hierin participeren bestuurders, (secretaris-)directeuren en Chief Digital Officers van waterschappen, alsmede afgevaardigden van de Unie van Waterschappen, Het Waterschapshuis en de STOWA.

In januari 2025 is door WSHD het Informatiebeveiliging Governance Plan[11] opgesteld. Het Governance-plan gaat in op o.a. procedures, compliance en audit, incidentbeheer, training en bewustwording, technologie en tools. De rollen en verantwoordelijkheden van de belangrijkste functies worden beschreven, met daarbij de opmerking dat voor enkele functies met inhuur gewerkt wordt. Tot slot wordt de aansturing en overlegstructuur van de organisatie weergegeven met daarin: Stuurgroep Veiligheid (maand), Strategisch Informatieveiligheid Overleg (kwartaal), Operationeel Security Overleg (week) en Tactisch Security Overleg (maand). Dit document heeft echter nog geen formele status en is ook nog niet geïmplementeerd.
Voor het vaststellen of en zo ja hoe getroffen maatregelen bijdragen aan de gewenste mate van informatieveiligheid wordt in het Governance Plan het instrument "KPI's" genoemd. Uitwerking en concrete invulling van deze "KPI's" heeft nog niet plaatsgevonden.

[10] Waterschap Hollandse Delta, *Strategisch Informatiebeveiligingsbeleid 2024 - 2026* (2024).
[11] Waterschap Hollandse Delta, *Informatiebeveiliging Governance Plan* (2025).

4.2 Governance bij WSHD

Bij WSHD is het Strategisch informatiebeveiligingsbeleid[10] de richtlijn voor bestuur, directie, afdelingshoofden, teamleiders en medewerkers die beschrijft hoe om te gaan met informatiebeveiliging.

WSHD hanteert volgens het Strategisch informatiebeveiligingsbeleid[10] de volgende belangrijke uitgangspunten voor informatiebeveiliging:

1. Bestuurders bevorderen een veilige werk cultuur.
2. De Secretaris-directeur is eindverantwoordelijk voor informatiebeveiliging, de inrichting en werking van de beveiliging.
3. Informatiebeveiliging is een verantwoordelijkheid van de gehele organisatie.
4. Alle processen, applicaties, gegevens en generieke infrastructuur (fysiek en informatie) hebben elk één formele eigenaar in de lijnorganisatie.
5. Informatiebeveiliging is risicomanagement en behoeft ook aandacht in (keten)samenwerking.
6. Het lijnmanagement is verantwoordelijk voor de beveiliging van hun informatie(systemen) volgens het 'pas toe of leg uit' principe.
7. Aandacht voor bewustwording en opleiding zijn een onmisbaar onderdeel van de inrichting van informatiebeveiliging.
8. WSHD hanteert als basisbeveiligingsniveau (BBN) BIO BBN2 dat voor nagenoeg alle informatie(systemen) een passende beveiliging biedt tegen beveiligingsincidenten.
9. WSHD heeft zich ten doel gesteld om te gaan acteren op volwassenheidsniveau 4 (BIO/AVG).

Het daadwerkelijk structureel uitvoeren van de beheersmaatregelen voor informatiebeveiliging wordt geborgd door de toewijzing van de rollen, coördinatie, beoordeling en implementatie van het beleid binnen de organisatie. Onderstaande taken en verantwoordelijkheden zijn vastgelegd in het informatiebeveiligingsbeleid.

College van Dijkgraaf en Heemraden

- Toezicht op het stelsel van informatiebeveiliging binnen WSHD
- Stelt het Informatiebeveiligingsbeleid voor informatiebeveiliging vast
- Bevorderen een veilige werk cultuur

Secretaris-Directeur

- Eindverantwoordelijk voor de werking en borging van informatiebeveiliging

Directie

- Draagt het informatiebeveiligingsbeleid uit
- Stelt relevantie van wet- en regelgeving vast
- Legt verantwoording af over het gevoerde beleid aan het College van D&H

Chief Information Security Officer (CISO)

- Onderhoudt het informatiebeveiligingsbeleid en onderliggende standaarden
- Coördineert de implementatie en beheersing van informatiebeveiliging
- Verspreidt het informatiebeveiligingsbeleid
- Monitort en rapporteert aan de directie
- Voert onafhankelijke controles uit op opzet, bestaan en werking van Informatiebeveiliging binnen WSHD
- Contactpersoon en vraagbaak m.b.t. informatiebeveiliging
- Geeft eveneens ongevraagd adviezen over informatiebeveiliging
- Onderhoudt contact met overheidsinstanties en speciale belangengroepen
- Stuurt de communicatie en bewustwording over informatiebeveiliging

Afdelingshoofd (algemeen)

- Invoeren en volgen van de richtlijnen in dit beleid
- Rapporteert over de invoering en werking van informatiebeveiliging aan de directie (lijnrapportage)
- Signaleert en meldt problemen en incidenten bij de CISO

Aan de VV is geen rol, taak of verantwoordelijkheid toegekend in het document Strategisch informatiebeveiligingsbeleid.

Tijdlijn besluitvorming aanpak cybersecurity
In onderstaande tabel zijn relevante beleidsdocumenten chronologisch opgenomen. Hierbij is in de kolom aangegeven welk gremium het document heeft vastgesteld.

Jaar	Unie van Waterschappen	Verenigde Vergadering	Dijkgraaf & Heemraden	Directie WSHD
2018	Aanvullende afspraken Bestuursakkoord Water			
2019				
2020				
2021		VV-voorstel bedrijfswaarden en bedrijfswaardenmatrix 3.0	Bestuurlijke informatiebrief 2021-13: stand van zaken Fysieke Toegangsbeveiliging	
2022		Trede 3 NEN-veiligheidsladder eind 2023 en Trede 4 AVG/BIO in 2024		
2023	Vaarkaart Digitale Transformatie			Strategisch Assetmanagementplan 2.0
2024		Managementletter	Jaarrapportage CISO/FG 2023 + collegevoorstel	Auditrapport BIO/AVG (Verdonck e.a.)
	Strategienota Digitale Transformatie Waterschappen		Strategisch Informatie beveiligingsbeleid	Governance informatiebeveiliging opgezet
		Trede 3 veiligheid behaald, volwassenheidniveau 4 eind 2025	Vervolg Veiligheid: trede 3 behaald, niveau 3 AVG/BIO in 2025 en niveau 4 in 2027	Start cybersecurity-team
		Doorleven trede 3, niveau 3 AVG/BIO in 2025 en niveau 4 in 2027		Kwartaalrapportages veiligheid Q1–Q3
2025	Handelingsperspectieven voor waterschappen bij risicovolle IT-afhankelijkheden	Informele VV; actuele stand van zaken cybersecurity	4-maands CISO/FG verslag	Kwartaalrapport Q4 2024
		Managementletter	Voortgangsrapport veiligheid Q1	Kwartaalrapport Q1 2025

Legenda:

Informatie	Besluit

Bevindingen en toetsing aan referentiekader

Bevinding 1	Het beleid en de strategie zijn vastgelegd in de volgende stukken: het Strategisch Informatiebeveiligingsbeleid 2024-2026 en het Informatiebeveiliging Governance Plan.
Referentiekader	Referentiekader D1 en D2.
Toetsing	✅ De norm vereist een formeel vastgesteld en geïmplementeerd ISMS. Het Strategisch Informatiebeveiligingsbeleid 2024-2026 is door D&H vastgesteld en het Informatiebeveiliging Governance Plan is door de directie vastgesteld.

Bevinding 2	De VV heeft van belang zijnde documenten voor cybersecurity niet vastgesteld. Tegelijkertijd heeft D&H deze documenten ook niet voorgelegd aan de VV.
Referentiekader	Referentiekader VV1 en DH1
Toetsing	❌ De norm vereist dat de VV (strategische) beleidsdocumenten vaststelt of minimaal hierover wordt geïnformeerd. Het niet voorleggen van het Strategisch Informatiebeveiligingsbeleid aan de VV is een tekortkoming in de voorbereidende - en verantwoordingsrol van D&H.

Bevinding 3	In zowel het Strategisch Informatiebeveiligingsbeleid als in het Governanceplan Informatiebeveiliging wordt de bestuurlijke positie van de VV niet vermeld.
Referentiekader	Referentiekader DH3 en VV2
Toetsing	❌ Het beleidskader geeft niet de volledige governancestructuur weer. Het ontbreken van de kaderstellende en controlerende rol van de VV is een fundamentele lacune in de beleidsarchitectuur. Met de aankomende cyberbeveiligingswet ligt de verantwoordelijkheid voor het beleid bij D&H . De naam 'Governanceplan informatiebeveiliging' impliceert een beschrijving van het bestuur, de beheersing en toezicht binnen de organisatie, maar is feitelijk een document dat de tactisch en operationele niveaus beschrijft gerelateerd aan de ambtelijke bedrijfsvoering. Er is geen vastlegging van de verantwoordelijkheidsverdeling tussen de VV en D&H.

Bevinding 4	Daar waar strategie en meerjarenthema's op de agenda van de VV aan de orde komen, is op geen enkele wijze aandacht geweest of aandacht gevraagd voor cybersecurity.
Referentiekader	Referentiekader VV1 en VV5

Toetsing	❌ De norm vereist dat de VV bij strategische beleidsvorming haar kaderstellende en controlerende rol actief vervult en cybersecurity als strategisch thema op de agenda plaatst.

Bevinding 5	In de begroting 2026 is cybercriminaliteit in de paragraaf Risico's Bestuur en Organisatie opgenomen als risico (Geen/beperkte toegang tot data/systemen door cybercriminaliteit) met een financieel gevolg van 500.000 en een kans van 25%. In het beschreven weerstandsvermogen is overigens geen rekening gehouden met de risico's Bestuur en Organisatie[12]. De in de programmabegroting (die door de VV wordt vastgesteld) opgenomen ambtelijke formatie is niet dusdanig gespecificeerd dat helder is welk budget voor cybersecurity beschikbaar is. Door het vaststellen van de begroting is dus impliciet budget voor cybersecurity beschikbaar gesteld door de VV.
Referentiekader	Referentiekader VV3 en D3
Toetsing	🟡 De norm vereist dat de VV budget ter beschikking stelt en de directie capaciteit organiseert voor het uitvoeren van het cybersecuritybeleid. Het is niet expliciet zichtbaar in de begroting, maar het beleid wordt wel uitgevoerd.

Bevinding 6	Uit interviews blijkt dat D&H training heeft gevolgd over cybersecurity en hun rol in het kader van de Cyberbeveiligingswet.
Referentiekader	Referentiekader DH6
Toetsing	✅. De leden van D&H hebben aantoonbaar een opleiding gevolgd op het gebied van cybersecurity.

[12] Waterschap Hollandse Delta, *Programmabegroting 2026, Meerjarenraming 2027 - 2030* (2025), par. Weerstandsvermogen en risicobeheersing, https://wshd.publicaties.app/pub/begroting2026/.

4.3 Risicobeheersing, maatregelen en uitvoering

Deelvraag 2 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?

Deelvraag 4 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?

WSHD gebruikt de bij het Waterschapshuis ontwikkelde systematische aanpak voor het identificeren en beoordelen van risico's die de informatiebeveiliging kunnen beïnvloeden (de zogenaamde Quickscan Object Classificaties). Op basis hiervan worden alle assets uit het watersysteem en uit de afvalwaterketen beoordeeld. Hierbij wordt onder andere gekeken naar de potentiële gevolgen van een hack. Op basis van die gevolgen wordt er door een team van deskundige medewerkers een benodigd "cybersecurity weerstandsniveau" bepaald. Dit risico-managementproces is samen met andere waterschappen en het Waterschapshuis ontwikkeld en gebruikt.

Risico's als gevolg van digitalisering[1] zijn:
- Cybercrime (aanvallen)
- Cyberspionage
- Cybersabotage

Als gevolg van een aanval kunnen effecten optreden voor de volksgezondheid, veiligheid, economie en ontwrichting van de samenleving.

WSHD beheert voor de afvalwaterketen o.a. 20 RWZI's, 1 slibverwerkingsinstallatie en 64 rioolgemalen. In een interview is aangegeven dat deze assets allemaal zijn voorzien van een individuele beoordeling. Vervolgens wordt gekeken of er bijzonderheden van toepassing zijn, zoals bijvoorbeeld ligging nabij kritieke entiteiten of gevoelige natuur. Na alle overwegingen door diverse specialisten worden de beoordelingen opgeleverd aan de cybersecurity experts van WSHD zodat per asset de juiste maatregelen in kaart gebracht kunnen worden. De Quickscan Object Classificatie van de RWZI Dordrecht en van de RWZI Hellevoetsluis zijn door de Rekenkamer als voorbeeld ingezien. Het team Waterketen heeft aan de hand van een door het Waterschapshuis ontwikkeld format, een individuele beoordeling uitgevoerd van de waterketen assets. Deze beoordeling was initieel uitgevoerd door een klein team (het assetteam). Na deze initiële beoordeling heeft er een brede review plaatsgevonden door experts binnen het programma waterketen. Na het verwerken van de input uit de review is de beoordeling vastgesteld. Deze beoordeling geeft inzicht in het benodigde weerstandsniveau t.a.v. de cybersecurity. De beoordeling, afgerond op 11 september 2025, is beschikbaar gesteld voor het onderzoek van de rekenkamer. De rekenkamer heeft geconstateerd dat het inzicht compleet is en dat risico's zijn beschreven en beheersmaatregelen zijn genoteerd.

Uit de Quickscan Object Classificaties blijkt dat de risico's die beoordeeld worden diverse invalshoeken betreffen zoals veiligheid medewerker / publiek (kans op gewonden), maatschappelijke gevolgen (effect op gebied / meer personen), financiële gevolgen (directe / herstel schade), domino-effect (uitval ander proces), ecologisch gevolg (omvang / herstel) en imago-schade (intern / lokaal / landelijk).

In 2026 wordt een nulmeting (impactanalyse) uitgevoerd waarbij in beeld wordt gebracht wat de huidige status is van de risicobeperkende maatregelen. Deze nulmeting wordt vervolgens vergeleken met de eerdergenoemde analyse van de assets. Op basis van de verschillen worden

maatregelen en investeringen opgenomen in de meerjarenprogrammering van het assetmanagementplan.

Naast de maatregelen per asset zijn er ook organisatorische maatregelen. Voor de bewustwording worden trainingen georganiseerd en ook worden audits door externe partijen uitgevoerd. Het signaleren, registreren en be- en afhandelen van incidenten en meldingen is volgens geïnterviewden ook een onderwerp dat permanente aandacht vergt. Immers: cybercriminelen ontwikkelen hun vaardigheden en instrumenten ook. In de organisatie zijn enkele overlegorganen (zoals de Stuurgroep Veiligheid, Strategisch veiligheidsoverwegingen en het Tactisch security overleg) in het leven geroepen. Van de overleggen worden geen verslagen bijgehouden, de Rekenkamer kan om die reden niet vaststellen wat daar wordt besproken en hoe de opvolging van de afspraken gaat.

De afhankelijkheid van de big-tech bedrijven uit Amerika wordt door het Waterschapshuis ook gezien als een risico. Vanuit het Waterschapshuis worden door de 21 waterschappen maatregelen genomen deze risico’s te mitigeren. In het door de Rekenkamer geraadpleegde vertrouwelijke document ‘Handelingsperspectieven voor de waterschappen bij risicovolle IT-afhankelijkheden’ wordt stilgestaan bij deze risico’s. Vanwege het vertrouwelijke karakter wordt in deze nota van bevindingen hier verder niet op ingegaan.

Uit interviews blijkt dat voor de medewerkers van WSHD door het jaar heen trainingen en bijeenkomsten voor alle medewerkers worden georganiseerd om de bewustwording te vergroten. Interviews geven aan dat men cybersecurity als een ”positieve belemmering” ziet: niet eenvoudig maar wel zeer noodzakelijk.

Tijdens locatiebezoeken aan Pernis en Hellevoetsluis gaven de buitendienst medewerkers duiding van de praktische werking van de beheersing van de cyberrisico's op de assets. De betrokken medewerkers bevestigden de deelname aan training en instructie op het gebied van cybersecurity.

Bevindingen en toetsing aan referentiekader

Bevinding 7	De organisatie heeft in 2024 en 2025 op het gebied van cybersecurity door middel van de risico-inventarisatie stappen gezet op het gebied van risicoanalyse en -beheersing. Met behulp van het Waterschapshuis is een wijze van samenwerking met collega-waterschappen opgezet. De implementatie van deze voor waterschappen eenduidige werkwijze inclusief de vereiste processen, is inmiddels gerealiseerd.
Referentiekader	Referentiekader D1
Toetsing	✅ De ingezette werkwijze via het Waterschapshuis sluit aan bij de norm voor een risicogerichte aanpak in het cybersecuritybeleid.

Bevinding 8	Eind 2025 is WSHD bij fysieke assets binnen de afvalwaterketen en het watersysteem gestart met inventarisatie van cyberrisico's en corresponderende maatregelen.
Referentiekader	Referentiekader D1
Toetsing	✅ Eind 2025 is WSHD bij fysieke assets binnen de afvalwaterketen en het watersysteem een vervolg gegeven aan de door het Waterschapshuis opgezette methode met de inventarisatie van cyberrisico's en corresponderende maatregelen..

Bevinding 9	De aanbevelingen (opgesomd in de CISO/FG rapportage 2023) als gevolg van (externe) audits zijn onvoldoende opgevolgd.
Referentiekader	Referentiekader DH2, DH5 en D4
Toetsing	❌ De norm vereist dat D&H toezicht houdt op de effectiviteit van maatregelen en de opvolging van aanbevelingen borgt. De 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 niet alles meteen opgevolgd worden. Onvoldoende opvolging duidt op een tekortkoming in zowel de sturing door de directie als het toezicht door D&H.

Bevinding 10	De VV wordt niet actief geïnformeerd over risico's of maatregelen als gevolg van cyberdreiging.
Referentiekader	Referentiekader DH4
Toetsing	❌ D&H schiet tekort in haar verantwoordingsplicht richting de VV, waardoor de VV haar controlerende rol niet kan invullen.

Bevinding 11	De medewerkers worden door middel van instructie uitgerust om risico's te beheersen.
Referentiekader	Referentiekader D4
Toetsing	✅ De organisatie van capaciteit en bewustwording van medewerkers sluit aan bij de aanpak in het cybersecuritybeleid.

4.4 Monitoring, evaluatie en externe validatie

Deelvraag 3 Hoe worden de rapportages over beheersing van de cyberrisico's extern gevalideerd?

Deelvraag 5: Hoe vindt monitoring en evaluatie van de maatregelen ter beheersing van de cybersecurityrisico's plaats?

4.4.1 Monitoring maatregelen

Monitoring vindt plaats op twee manieren: monitoring van de maatregelen ter beheersing van de risico's en monitoring van het behalen van trede's op de veiligheids- en volwassenheidsladder.

Monitoring maatregelen ter beheersing cyberrisico's

Voor procesautomatisering gelden algemeen van toepassing zijnde protocollen voor gebruik wachtwoorden en toegang tot informatiesystemen. Fysieke en functionele toegang worden toegekend op basis van de functie en bevoegdheden van medewerkers. Het gebruik van deze toegangsmogelijkheden wordt 24/7 gemonitord en geregistreerd in logging. Afwijkingen worden geconstateerd en opgevolgd. In de processen van de IT-afdeling is dit geïmplementeerd en de CISO/FG-functies beschouwen aanvullend hoe deze processen verlopen en of aanvullende actie nodig is.

De monitoring van de genomen maatregelen in het kader van cybersecurity gebeurt vanuit de Waterschapsbrede regiekamer. De parameters van alle assets (zoals het debiet (aan- en afvoer), waterniveau, zuurstofgehalte, pH waarde, temperatuur e.d.), maar ook de installatiestatus (b.v. staan de pompen aan/uit, energieverbruik en storingsmeldingen) kunnen realtime en op afstand worden uitgelezen. Afwijkingen worden meteen gesignaleerd. Afwijkingen van deze parameters kunnen duiden op het optreden van een cyberrisico zoals ongeoorloofde aansturing of beïnvloeding van de assets.

Monitoring van ongeoorloofde pogingen om toegang te verkrijgen tot de aansturing van systemen gebeurt via SIEM-systemen. Het SIEM-systeem analyseert patronen en slaat alarm bij afwijkend gedrag, zoals herhaalde mislukte inlogpogingen.

Buitendienstmedewerkers kunnen ook op afstand via een tablet de assets monitoren. Om toegang te verkrijgen tot de bedieningssoftware zijn op diverse niveaus veiligheidsmaatregelen genomen om onbevoegde toegang te voorkomen.

Afwijkingen van de parameters worden realtime gerapporteerd. De organisatie van WSHD is ingericht om meteen te kunnen acteren.

Monitoring trede 3 veiligheidsladder en trede 4 volwassenheidsniveau

Monitoring vindt primair plaats door de directe verantwoordelijke medewerkers, de CISO en de Functionaris Gegevensbescherming (FG). De extern accountant beschrijft in zijn managementletter welke punten bij de accountantscontrole zijn opgevallen. Zo maakt de accountant in de managementletter 2024 [13] opmerkingen over het achterblijven van maatregelen n.a.v. een ethical hacking, het monitoren van verbeterpunten uit een cyberweerbaarheidsscan uit augustus 2023 en het op een andere manier positioneren van de CISO in de organisatie. In de managementletter 2025 [14] komt de accountant hierop terug en constateert dat er opvolging is gegeven aan de aanbevelingen, maar dat op het gebied van volwassenheidsniveau 4 en positionering van de CISO onvoldoende stappen zijn gemaakt. De accountant adviseert om blijvend aandacht te besteden aan de nieuwe wetgeving (Cyberbeveiligingswet).

[13] Waterschap Hollandse Delta, *Programmabegroting 2026, Meerjarenraming 2027 - 2030*, par. Weerstandsvermogen en risicobeheersing.Publieke Sector Accountants, *Managementletter 2024* (2024).
[14] Publieke Sector Accountants, *Managementletter 2025 - concept* (z.d.).

Uitgangspunt voor monitoring en bepalen van de stand van zaken op het gebied van informatieveiligheid en privacy is het volwassenheidsniveau dat bereikt is.

4.4.2 Audit

Eind 2023 is in een audit voor alle waterschappen door Verdonck, Klooster en Associates[15] het niveau van het inmiddels bereikte volwassenheidsniveau gemeten. Voor WSHD is daarbij vastgesteld dat gemiddeld onder Niveau 3 (zie bijlage 3) gescoord is. Deze audit is een eerste 'validatie' van de huidige status van informatieveiligheid, privacy en het managementsysteem.

De extern accountant heeft in zijn Managementletter 2024 [13] en 2025 [14] gerapporteerd over IT-veiligheidsaspecten, zij het dat dit vooral gelinkt is met financiële verantwoordingsaspecten. Voor het opvolgen van actiepunten n.a.v. een ethical hacking-test, de onafhankelijke positie van de CISO en de verbeterpunten om door te groeien naar volwassenheidsniveau 4 vraagt de accountant aandacht.

Externe audits en penetratietesten worden ook uitgevoerd en hier is het Waterschapshuis ook veelal partij bij als opdrachtgever of projectleider. In dat geval zijn meer waterschappen onderwerp van de audit.
De rapportages van door externe bureaus uitgevoerde specifieke audits zijn wel beschikbaar, maar worden niet aan het College van D&H of aan de VV aangeleverd.

Bevindingen en toetsing aan referentiekader

Bevinding 12	De bevindingen van de audit Verdonck, Klooster en Associates waren gemiddeld genomen onder het beoogde volwassenheidsniveau.
Referentiekader	Referentiekader DH2, DH4, DH5, D4
Toetsing	❌ De directie heeft onvoldoende gestuurd op het behalen van de eigen doelstellingen. D&H had hierop moeten ingrijpen.

Bevinding 13	Externe validatie van cybersecurityrapportages wordt ingevuld door audits. De externe accountant van WSHD beoordeelt de beveiliging van de IT-omgeving en de organisatie rond informatiebeveiliging.
Referentiekader	Referentiekader DH2, DH5 en C2
Toetsing	✅ De inzet van externe audits en accountantscontrole als validatie-instrument sluit aan bij de norm.

Bevinding 14	De opvolging van de geconstateerde actiepunten is voor het bestuur te onzichtbaar. De CISO vraagt daar in zijn rapportages met regelmaat aandacht voor.
Referentiekader	Referentiekader DH2, D4

[15] Verdonck, Klooster & Associates, *Waterschap Hollandse Delta- Auditrapport Integrale BIO/AVG audit* (2024).

Toetsing	❌ Het is zorgelijk dat de CISO herhaaldelijk moet vragen om aandacht voor opvolging. D&H en directie zijn verantwoordelijk voor actieve sturing op actiepunten.

Bevinding 15	Bevindingen worden opgenomen in rapportages van de CISO/FG.
Referentiekader	Referentiekader C2
Toetsing	✅ De CISO vervult zijn rapporterende taak.

Bevinding 16	Het college van D&H wordt niet altijd in kennis gesteld van externe auditrapporten.
Referentiekader	Referentiekader D4
Toetsing	🟡 De norm vereist dat D&H als eindverantwoordelijk bestuur kennis heeft van externe audituitkomsten. De auditrapportages AVG-BIO zijn wel gedeeld, maar het rapport van Verdonck, Klooster en Associates niet. Het niet doorgeleiden van alle auditrapporten naar D&H is een tekortkoming van de directie.

Bevinding 17	De VV heeft geen zicht op de externe auditrapporten over cybersecurity, afgezien van de managementletter van de accountant.
Referentiekader	Referentiekader DH4
Toetsing	❌ de VV wordt door D&H geïnformeerd via informatieve VV bijeenkomsten. Er bestaat geen formele rapportagelijn. D&H legt onvoldoende verantwoording af. De VV beschikt daardoor niet over de informatie die nodig is voor een adequate controlerende rol.

Bevinding 18	Monitoring van de maatregelen ter beheersing van de cybersecurityrisico's vindt plaats via de Waterschapsbrede regiekamer.
Referentiekader	Referentiekader D1
Toetsing	✅ Technische monitoring is aanwezig en functioneert.

Bevinding 19	Evaluatie van de maatregelen gebeurt via rapportages aan directie en bestuur.

Referentiekader	Referentiekader C2
Toetsing	✅ De rapportagecyclus is ingericht.

Bevinding 20	Rapportages van de CISO en FG komen niet bij de VV terecht.
Referentiekader	Referentiekader DH2
Toetsing	❌ D&H draagt onvoldoende zorg voor het doorgeleiden van relevante informatie naar de VV, waardoor de controlerende rol van de VV wordt belemmerd.

Bevinding 21	Bespreking van CISO-jaarrapportage over 2024 (d.d. 15 januari 2025), met daarin kritische kanttekeningen is 8 maanden later in het college van D&H besproken op 16 september 2025.
Referentiekader	Referentiekader DH2
Toetsing	❌ De norm vereist dat D&H tijdig kennisneemt van rapportages. Een doorlooptijd van 8 maanden voor bespreking van een jaarrapportage getuigt niet van actief en tijdig toezicht.

Bevinding 22	De aanbevelingen uit externe (b.v. de Klooster & Verdonck audit en de aanbevelingen van de accountant) en interne rapportages c.q. actiepunten (uit CISO rapporten) worden niet actueel gemonitord en opgevolgd, waardoor niet realtime zichtbaar is wat de stand van zaken bij die externe en interne actiepunten is.
Referentiekader	Referentiekader DH2, D2 en D4
Toetsing	❌ De norm vereist actieve en tijdige rapportage over de uitvoering van het cybersecuritybeleid. Het ontbreken van een actueel overzicht is een structurele tekortkoming.

Bevinding 23	De door de extern accountant in zijn managementletter tot tweemaal toe gemaakte opmerking “dat de positie van de CISO zijn onafhankelijkheid belemmerd” heeft geleid tot herpositionering in de organisatie van de CISO (van afdeling informatie & automatisering naar concernstaf).
Referentiekader	Referentiekader DH3, D1 en C1

Toetsing	✅ De herpositionering sluit aan bij de norm voor een onafhankelijke positie van de CISO. Dit is een positieve ontwikkeling, al was sturing vanuit D&H eerder gewenst geweest.

Bevinding 24	De VV heeft geen vragen gesteld, geen moties ingediend en geen agenderingsverzoek gedaan over monitoring en evaluatie van maatregelen ter beheersing van de cybersecurityrisico's.
Referentiekader	Referentiekader VV4 en VV5
Toetsing	❌ De VV maakt geen gebruik van haar bestuurlijke instrumentarium op dit terrein.

4.5 Bestuurlijke informatievoorziening en rol van de VV

Deelvraag 6 Welke informatie ontvangen de leden van de VV over cybersecurityrisico's en de bijbehorende beheersmaatregelen?

Strategische documenten zoals het Strategisch Assetmanagementplan[16] en het Strategisch Informatiebeveiligingsbeleid[10] zijn respectievelijk door de directie of door het college van D&H vastgesteld. De VV is niet gevraagd deze stukken vast te stellen.

Het vaststellen van de ambitie om per 1 januari 2024 trede 3 van de veiligheidsladder en trede 4 volwassenheidsniveau AVG/BIO in 2024 te bereiken is in juni 2022 door de VV vastgesteld. Het niet behalen van deze ambitie en het verschuiven van de deadline om beide niveaus te behalen, is door middel van een VV-info[17] gerapporteerd aan de VV. In november 2024 rapporteert D&H dat volwassenheidsniveau 4 eind 2025 wordt verwacht. In dezelfde maand neemt D&H het besluit volwassenheidsniveau 4 in 2027 te behalen. De VV wordt hierover in december 2024 middels een VV-info[18] geïnformeerd. De VV neemt deze verschuivingen in de deadline voor kennisgeving aan.

De VV wordt in algemene termen (bijvoorbeeld uit VV-info 2024-33: "*Op onderdelen is het risico niet gedaald en in een aantal gevallen licht gestegen.*") en op onregelmatige basis geïnformeerd over cybersecurityrisico's en beheersmaatregelen. De VV wordt met name geïnformeerd door middel van informatiebrieven over de trede op de NEN-veiligheidsladder en van het volwassenheidsniveau AVG/BIO.

Daarnaast wordt af en toe een presentatie in een informatieve VV georganiseerd. Op 28 mei 2025 is onder meer de ontwikkeling van de afgelopen jaren geschetst en de aanpassing van het cybersecurity-team in 2024 aangekondigd.

In de P&C-documenten wordt cybersecurity niet als thema weergegeven en alleen zijdelings genoemd indien er een financieel aspect aan de orde is. Jaarstukken en begrotingsdocumenten 2024 geven geen overzicht van de status van cybersecurity.

[16] Waterschap Hollandse Delta, *Strategisch Assetmanagement Plan 2.0* (2022).
[17] Waterschap Hollandse Delta, *VV-info 2024-33 - Stand van zaken Veiligheid: Volwassenheidsniveau (Informatieveiligheid en Privacy) en Veiligheidscultuurladder (Mens- en Objectveiligheid), SCL Ladder trede 3 behaald!* (2024).
[18] Waterschap Hollandse Delta, *VV-info 2024-37 - Vervolg stand van zaken Veiligheid* (2024).

Alle VV leden zijn in 2025 door het Waterschapshuis uitgenodigd om een presentatie over cybersecurity bij te wonen. Vanuit de VV van WSHD hebben 4 leden zich aangemeld. Als gevolg van geringe belangstelling is de presentatie niet doorgegaan.

Uit interviews blijkt dat de ambtelijke organisatie zoekende is naar de manier waarop het bestuur betrokken wil worden en haar bestuurlijke verantwoordelijkheid waar kan maken.

Uit het raadplegen van het bestuurlijk informatiesysteem blijkt dat VV leden bij het college van D&H geen informatie hebben opgevraagd of vragen gesteld over cybersecurity.

Uit de enquête onder VV-leden blijkt dat:

1. de meeste VV leden de doelstellingen over het te behalen veiligheidsniveau en volwassenheidsniveau niet exact kennen;
2. de meeste VV leden D&H op hoofdlijnen controleert op het uitgevoerde risicobeheersingsbeleid;
3. de helft van de respondenten via rapportages en voorstellen betrokken wenst te worden bij de sturing op cybersecurityrisico's;
4. de helft van de respondenten aangeeft bestuurlijke instrumenten (zoals schriftelijke vragen, moties en agenderingsverzoeken) in te zetten op het onderwerp risicobeheersing van de cyberdreiging.

De leden van de klankbordgroep uit de VV gaven aan dat het wenselijk is beter geïnformeerd te worden over beheersing van de cybersecurityrisico's op de assets van het waterschap. Hierbij is het volgende aangegeven:

1. Open bespreking welke risico's er zijn en hoe we deze kunnen bestrijden.
2. Het AB heeft inzicht nodig in de belangrijkste risico's, hoe goed de beveiliging werkt, is er al wat misgegaan. Wat als het volledige systeem plat gaat door een hack voor meerdere dagen.
3. Inzage jaarlijkse rapportages cybersecurityrisico's assets, organisatie algemeen en ICT-afdeling.
4. Meenemen in de bestuurlijke nieuwsbrieven
5. Tussentijdse rapportering, maar niet op detailniveau.
6. technische stand van de assets en modus operandi (handbediening mogelijk etc.)

De resultaten van de enquête zijn toegevoegd als bijlage 2 aan dit rapport.

Bevindingen en toetsing aan referentiekader

Bevinding 25	De informatie naar de VV gaat vooral over de positie op de NEN-veiligheidsladder en de stand van het volwassenheidsniveau AVG/BIO.
Referentiekader	Referentiekader DH2 en DH4
Toetsing	❌ D&H legt gestructureerd en volledig verantwoording af aan de VV over o.a. externe audits, uitkomsten van CISO/FG rapportages en opvolging van aanbevelingen daarvan. Informatie uitsluitend over de positie op de veiligheidsladder is onvoldoende voor een adequate controlefunctie van de VV.

Bevinding 26	De VV is over de positie op de NEN-veiligheidsladder en de stand van het volwassenheidsniveau AVG/BIO op onregelmatige basis middels informatiebrieven en op onregelmatige informatiesessies mondeling geïnformeerd.

Referentiekader	Referentiekader DH2
Toetsing	🟡 D&H verstrekt structurele, periodieke verantwoording aan de VV. Hoewel er wel wordt gerapporteerd, is dit echter onregelmatig. Van een gestructureerde verantwoording is geen sprake.

Bevinding 27	Leden van de VV zijn uitgenodigd geweest door het Waterschapshuis om bijgepraat te worden over cybersecurity. Er hebben zich slechts 4 leden van de VV van WSHD aangemeld. Als gevolg van de geringe belangstelling ging de presentatie niet door.
Referentiekader	Referentiekader VV5
Toetsing	❌ Om haar controlerende rol en versterking van de informatiepositie waar te kunnen maken dient de VV zich goed te laten informeren.

Bevinding 28	Leden van de VV geven in de enquête aan bestuurlijke instrumenten in te zetten op het onderwerp cybersecurity. Dit blijkt niet uit de opgevraagde stukken.
Referentiekader	Referentiekader VV5
Toetsing	🟡 Er is bewustzijn bij leden van de VV, maar de vertaling naar daadwerkelijk bestuurlijk handelen ontbreekt.

Bevinding 29	Leden van de VV hebben nadrukkelijke wens om meer betrokken te worden bij het onderwerp cybersecurity.
Referentiekader	Referentiekader VV1 en DH2
Toetsing	🟡 De wens van VV-leden biedt aanknopingspunten voor verbetering van de betrokkenheid bij het cybersecuritybeleid. D&H heeft hier een kans om op in te spelen.

Bevinding 30	Leden van de VV zijn nog niet door organisatie, noch door D&H gevraagd of en zo ja welke rol ze wensen te hebben op het terrein van cybersecurity (of over welk ander strategisch onderwerp dan ook).
Referentiekader	Referentiekader DH2
Toetsing	❌ D&H heeft de VV niet actief betrokken bij de afbakening van haar rol.

Referenties

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2), EUR-lex 80 (2022). http://data.europa.eu/eli/dir/2022/2555/oj.

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing, Legislation No. 32022L2557, EUR-Lex (2022). http://data.europa.eu/eli/dir/2022/2557/oj.

Publieke Sector Accountants. *Managementletter 2024*. 2024.

Publieke Sector Accountants. *Managementletter 2025 - concept*. z.d.

Rijksoverheid, Vereniging van Nederlandse Gemeenten, Interprovinciaal Overleg, en Unie van Waterschappen. *BASELINE INFORMATIEBEVEILIGING OVERHEID 2 - BIO 2*. 2026.

Rijkswaterstaat en Het Waterschapshuis. *Cybersecurity Implementatierichtlijn Objecten*. Versie 3.4. 2021. https://cuatro.sim-cdn.nl/certwm/uploads/csir-3.4-definitief-concept-20210914.pdf?cb=eKtH4fdi.

Unie van Waterschappen. *Aanvullende afspraken Bestuursakkoord Water*. 2018. https://unievanwaterschappen.nl/wp-content/uploads/2021/11/Toekomstvisie-Bestuursakkoord-Water-2018.pdf.

Verdonck, Klooster & Associates. *Waterschap Hollandse Delta- Auditrapport Integrale BIO/AVG audit*. 2024.

Waterschap Hollandse Delta. *Informatiebeveiliging Governance Plan*. 2025.

Waterschap Hollandse Delta. *Programmabegroting 2026, Meerjarenraming 2027 - 2030*. 2025. https://wshd.publicaties.app/pub/begroting2026/.

Waterschap Hollandse Delta. *Reglement van Orde VV WSHD 2025*. 2025. https://lokaleregelgeving.overheid.nl/CVDR745840/1.

Waterschap Hollandse Delta. *Strategisch Assetmanagement Plan 2.0*. 2022.

Waterschap Hollandse Delta. *Strategisch Informatiebeveiligingsbeleid 2024 - 2026*. 2024.

Waterschap Hollandse Delta. *VV-info 2024-33 - Stand van zaken Veiligheid: Volwassenheidsniveau (Informatieveiligheid en Privacy) en Veiligheidscultuurladder (Mens- en Objectveiligheid), SCL Ladder trede 3 behaald!* 2024.

Waterschap Hollandse Delta. *VV-info 2024-37 - Vervolg stand van zaken Veiligheid*. 2024.

Waterschapswet (2024). https://wetten.overheid.nl/BWBR0005108/2026-01-01.

Wet weerbaarheid kritieke entiteiten, Staatsblad 2026, 188 (2026). https://zoek.officielebekendmakingen.nl/stb-2026-188.html.

Bijlage 1. Geïnterviewde functionarissen

Met enkele functionarissen is meerdere keren gesproken.

Intern
- Directielid
- Chief Information Security Officer (CISO)
- Afdelingshoofd I&A
- Functionaris Gegevensbescherming (FG)
- Secretaris-directeur
- Assetmanager waterketen
- Assetmanager watersysteem
- vml. Domeinmanager veiligheid
- Tactisch systems engineer waterketen
- Technisch beheerder gemaal Poortugaal
- Technisch beheerder rioolwaterzuivering Hellevoetsluis
- Projectmanager Technische Automatisering
- Verantwoordelijk heemraad
- VV-leden

Extern
- Omgevingsmanager Informatieveiligheid en Privacy (Waterschapshuis)

Bijlage 2. Enquête voor klankbordgroep

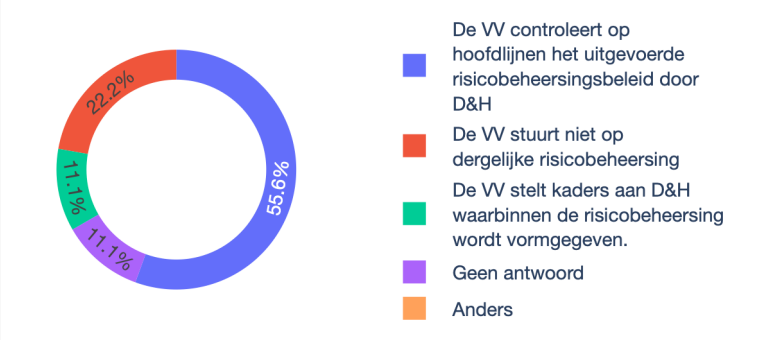
1. Wordt u als VV lid betrokken bij de cyber-risicobeheersing van de assets van het waterschap?



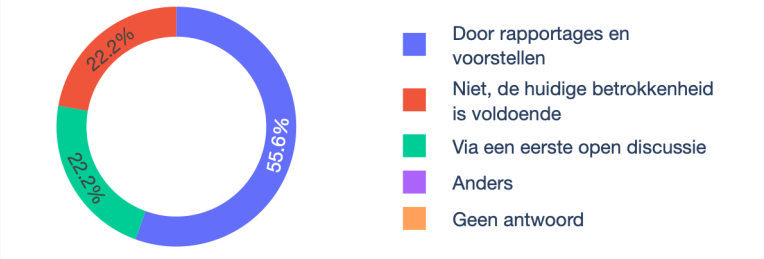
2. Wat weet u van de ambities en doelstellingen die door WSHD zijn gesteld over cyberveiligheid?



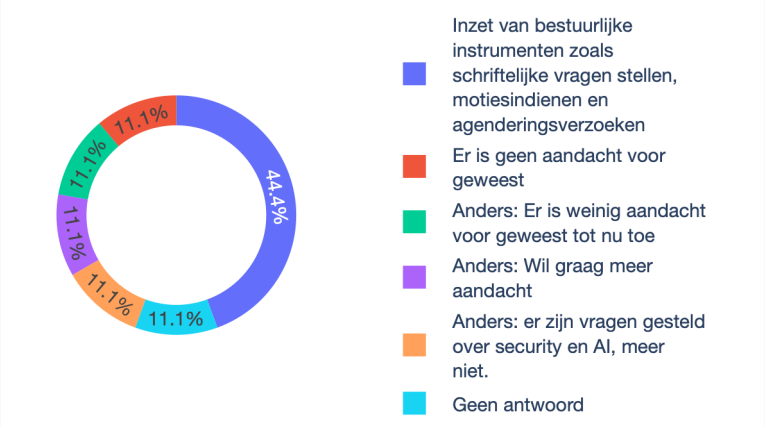
3. Hoe wordt de VV in staat gesteld om te kunnen sturen op cyber- risicobeheersing van de assets (zoals rwzi's, gemalen en sluizen)?



4. Hoe zou u betrokken willen worden bij de sturing op cybersecurityrisico's?



5. Welke aandacht is er vanuit de VV geweest voor risicobeheersing van de cyberdreiging op de assets?



6. Wat heeft u nodig om (nog) beter geïnformeerd te worden over beheersing van de cybersecurityrisico's op de assets van het waterschap? Open vraag

- Open bespreking welke risico’s er zijn en hoe we deze kunnen bestrijden.
- Het AB heeft inzicht nodig in de belangrijkste risico’s, hoe goed de beveiliging werkt, is er al wat misgegaan. Wat als het volledige systeem plat gaat door een hack voor meerdere dagen.
- Inzage jaarlijkse rapportages cybersecurityrisico's assets, organisatie algemeen en ict-afdeling.
- Meenemen in de bestuurlijke nieuwsbrieven
- Tussentijdse rapportering, maar niet op detailniveau.
- technische stand vd assets en modus operandi (handbediening mogelijk etc)

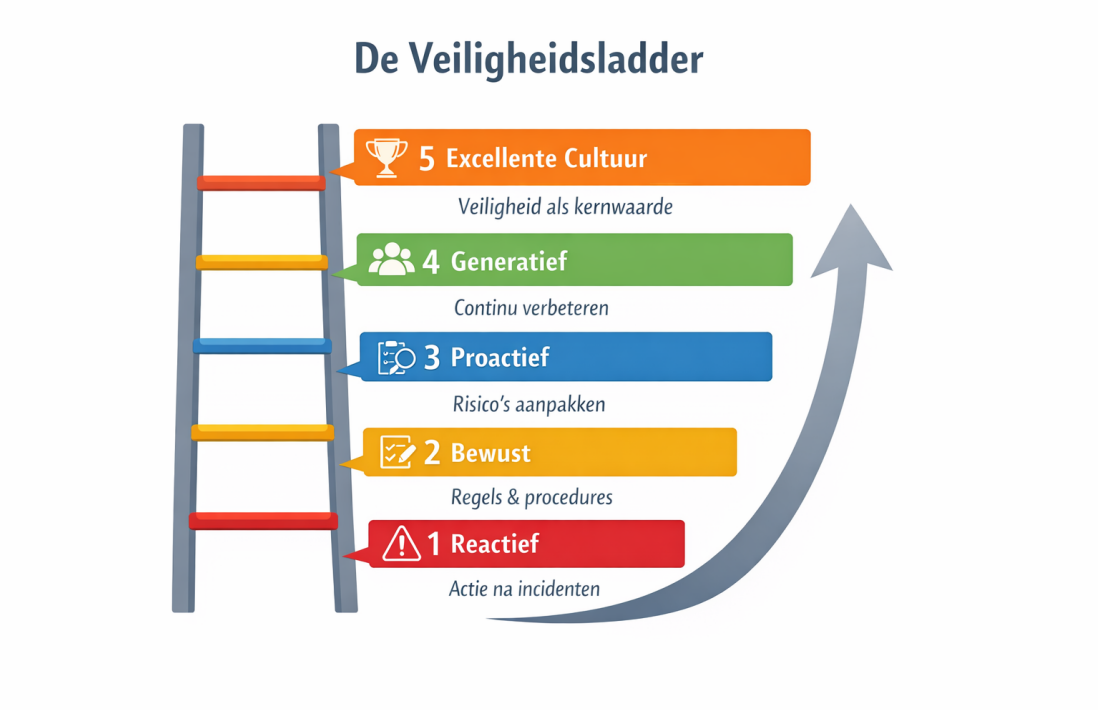
7. Wilt u de rekenkamer nog iets meegeven voor dit onderzoek?

- Onderzoek of de governance en verantwoordelijkheden duidelijk zijn, gebruik de bekende normen BIO/ISO voor objectiviteit. Kijk naar de praktijk (is er een simulatie mogelijk), leverancierssketens, analyseer recente incidenten…….is het onderdeel van de goed geteste calamiteiten procedure. Kijk of een professionele hacker het systeem kan kraken, d.w.z. het bloot leggen van ‘achterdeurtjes’
- Kritisch blijven en het een beetje laten schuren
- Bewustwording is een isme/. Uitvoering en implementering is voor organisatie

Bijlage 3: Veiligheidsladder en BIO-SA volwassenheidsmodel

De Veiligheidsladder is ontwikkeld door TNO (Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek) in samenwerking met verschillende industriële en overheidspartners. Het doel van de veiligheidsladder is een objectief meetinstrument te bieden om de veiligheidscultuur van een organisatie te beoordelen, vooral op het gebied van procesveiligheid en gedragsveiligheid.

Het concept is gebaseerd op internationale inzichten in veiligheidsmanagementsystemen, maar de uitwerking en certificeringsmethode zijn Nederlandse ontwikkeling.



Het BIO-SA volwassenheidsniveau kent 5 niveaus om te meten hoe volwassen de organisatie omgaat met informatiebeveiliging. De niveaus zijn ingedeeld volgens onderstaand schema.

