Onderzoeksvoorstel ‘cyber security’

Datum: 2 juni 2025

Status: definitief

---

1 Aanleiding en doel van het onderzoek

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.

De rekenkamer wil met deze quickscan 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.

2 Onderzoeksvragen

2.1 Hoofdvraag

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?

2.2 Deelvragen:

1. Wat is het beleid en strategie omtrent cybersecurity bij de WSHD?
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?
3. Hoe worden de rapportages over beheersing van de cybersecurityrisico’s extern gevalideerd?
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?
5. Hoe vindt monitoring en evaluatie van deze maatregelen plaats?
6. Welke informatievoorziening ontvangen de leden van de Verenigde Vergadering over cybersecurityrisico’s en de hierbij behorende beheersmaatregelen?

3 Afbakening

Dit onderzoek richt zich op de digitale risico’s voor de bediening van de assets (zoals gemalen, sluizen e.d.) in de primaire processen (niet zijnde kantoorautomatisering) en de beheersmaatregelen (inclusief gedragingen door gebruikers) die door het waterschap worden

genomen. Het onderzoek is verkennend van aard (quickscan) en kent geen diepgaande technische audit.

4 Onderzoeksmethoden

4.1 Documentanalyse

Analyse van relevante interne documenten zoals:

- Informatiebeveiligingsbeleid / -strategie voor assets
- Risicorapportages (zoals weerbaarheidsscans)
- Interne audits / ENSIA-rapportages[1]
- Notulen en stukken voor de Verenigde Vergadering en waterschapscommissies met betrekking tot informatieveiligheid
- Managementletter van de controlerende accountant

4.2 Interviews

Korte interviews met sleutelfunctionarissen:

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- IT-manager
- Functionaris Gegevensbescherming (FG)
- Secretaris-directeur
- Medewerkers die omgaan met risicovolle assets
- Verantwoordelijk(e) heemra(a)d(en)
- Fractievoorzitters (en/of leden klankbordgroep) van de Verenigde Vergadering

4.3 Vergelijking met normen en good practices

Gebruik van standaarden zoals BIO (Baseline Informatiebeveiliging Overheid), NCSC-adviezen[2], NEN-ISO/IEC 27001[3] en NEN-ISO/IEC 27002 [4] en NIS2 [5] . Toepassing van ‘good practices’ en beheersmaatregelen uit andere overheidsorganen als referentie.

5 Verwachte risico’s / aandachtspunten

De volgende risico’s worden mogelijk verkend (onder voorbehoud van vaststelling tijdens het onderzoek):

---

[1] ENSIA staat voor Eenduidige Normatiek Single Information Audit. Het is een systematiek die overheidsorganisaties helpt om verantwoording af te leggen over hun informatiebeveiliging.
[2] Het NCSC is een onderdeel van het ministerie van Justitie en Veiligheid en valt onder de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).
[3] ISO 27001 is een wereldwijd erkende norm op het gebied van informatiebeveiliging
[4] NEN-ISO/IEC 27002:2023 – Informatiebeveiliging, Cybersecurity en Bescherming van Privacy – Praktische richtlijnen voor informatiebeveiligingsmaatregelen
[5] NIS2 staat voor 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.

- Onvoldoende inzicht in actuele dreigingen;
- Afwezigheid of onvolledigheid van risico-inventarisatie;
- Beperkte capaciteit voor structurele monitoring;
- Beperkte kennis/alertheid binnen de organisatie;
- Beperkte kennis/alertheid binnen bestuur;
- Informatievoorziening aan de VV onvoldoende gestructureerd of incidentgedreven.

6 Verwachte resultaten en rapportage

De quickscan resulteert in een korte rapportage met:

1. Een beschrijving van de huidige stand van zaken
2. Een overzicht van de belangrijkste risico's en hoe deze worden beheerst
3. Een beoordeling van de mate van betrokkenheid en informatievoorziening aan de Verenigde Vergadering
4. Aanbevelingen voor versterking van risicobeheersing en bestuurlijke informatievoorziening

7 Indicatieve planning

Fase	Periode
Voorbereiding & opstart	Mei 2025
Documentanalyse	Mei 2025
Interviews	Juni 2025
Analyse en rapportage	Juli 2025
Voorlegging conceptrapport	September 2025
Eindrapportage	Oktober 2025

8 Opmerkingen

Dit onderzoek is een verkennende quickscan die wordt uitgevoerd door de leden van de rekenkamer zelf en vormt mogelijk de opmaat naar een verdiepend vervolgonderzoek.

De rekenkamer kan indien gewenst samenwerken met externe deskundigen op het gebied van informatiebeveiliging.