

De route naar groei

Uitwerking volwassenheidsniveau 4
in de waterschapssector

Versie 1.02

September 2023



Inleidend

- De waterschappen willen een betrouwbare, toegankelijke overheid zijn, daar hoort bij dat de belangen en gegevens van betrokkenen goed beschermd worden
- Waterschappen moeten daarvoor volwassen zijn in de omgang met en de beveiliging van (persoons-)gegevens en objecten, assets en systemen
- Waterschappen hebben behoefte aan een eenduidige en toepasbare uitwerking van het beoogde volwassenheidsniveau
 - In de discussie over de cijfers 3 en 4 gaat de bedoeling nog wel eens verloren
- Volwassenheid gaat niet over het zetten van vinkjes op een checklist
- Volwassenheid gaat over kritisch blijven kijken naar je organisatie en haar omgeving
- Een volwassen organisatie op niveau 4:
 - opereert risicogestuurd (denken – werken – sturen),
 - maakt bewuste keuzes met betrekking tot prioriteren van maatregelen,
 - blijft de effectiviteit van de maatregelen meten, beoordelen en verbeteren waar nodig.

Uitgangspunten

- De afspraak om ambitieniveau 4 te behalen staat niet ter discussie, deze uitwerking schetst het eindbeeld van een volwassen organisatie
- Deze uitwerking vormt een concretisering van dit niveau:
 - wat is de bedoeling, de essentie?
- Uitwerking focust op het "wat", niet op het "hoe", er is implementatieruimte voor de waterschappen
- Uitwerking blijft in lijn met eerdere uitleg en geadviseerde modellen
- En in lijn met bestaande en nieuwe nationale en Europese wetgeving (AVG, Wbni, NIS2, CER)
- Met aandacht voor aantoonbaarheid in de audit, met name op de werking

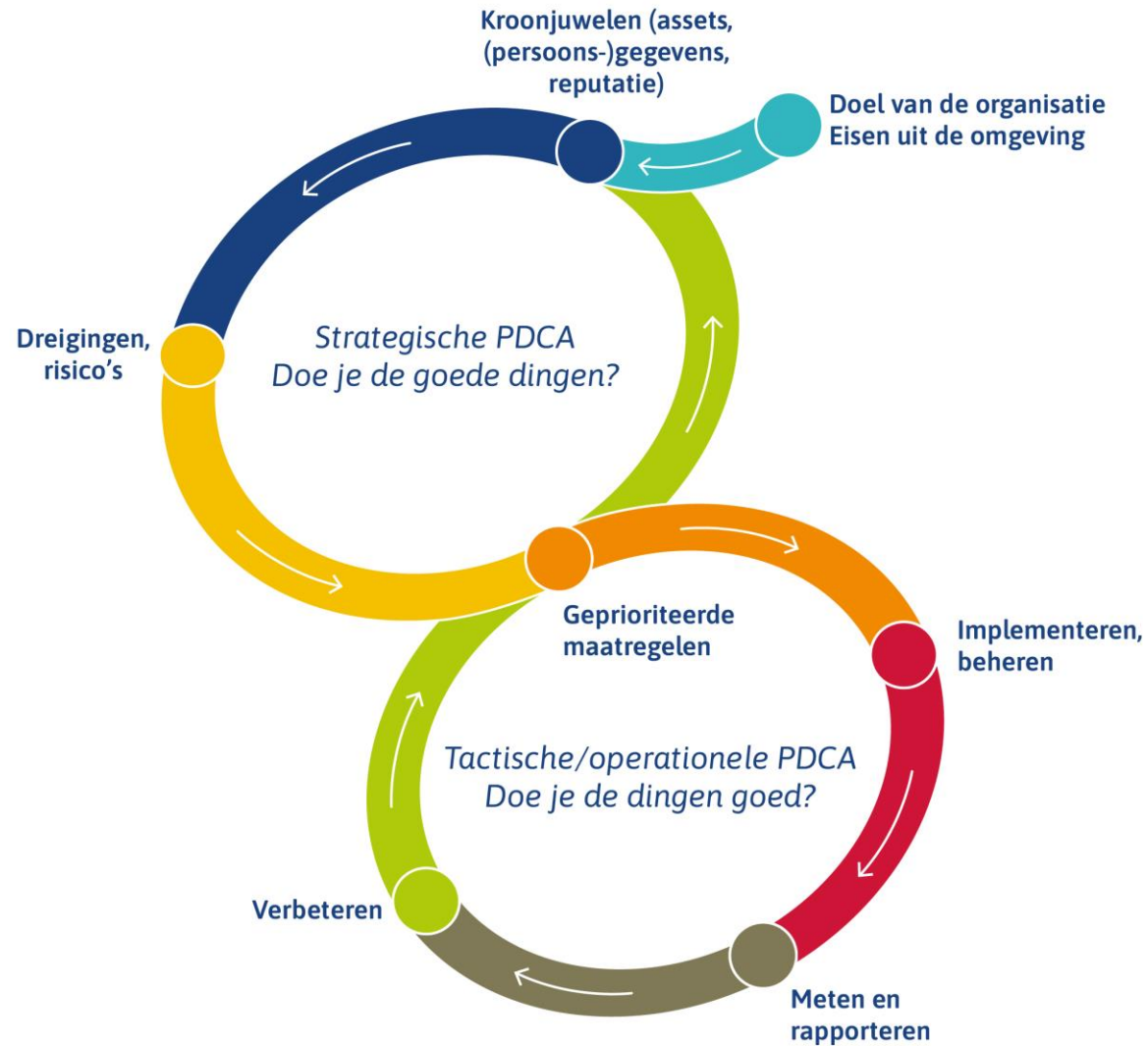
Beoordelingscriteria



Animatie volwassenheidsniveau 4



Volwassenheid gevisualiseerd



Beoordelingscriteria, risicomanagement

De organisatie:

- heeft inzichtelijk wat haar doelen zijn en de eisen die de omgeving aan haar stelt
- heeft bepaald welke kroonjuwelen essentieel zijn voor het bereiken van de doelen (objectclassificatie, dataclassificatie, procesclassificatie, gevoeligheid van persoonsgegevens)
- heeft een actueel dreigingsbeeld dat als input wordt gebruikt voor de risicoanalyse
- heeft haar risicobereidheid vastgesteld
- heeft middels een risicoanalyse de risico's vastgesteld, maatregelen geprioriteerd en de restrisico's geaccepteerd



Beoordelingscriteria, pdca-cyclus

De organisatie:

- Heeft in beginsel alle maatregelen uit de relevante baselines (BIO, AVG, IEC62443) geïmplementeerd:
 - Verantwoording van keuzes (comply-or-explain) gebaseerd op de risicoanalyse, vastgelegd in de Verklaring van toepasselijkheid
- Bepaalt voor de geprioriteerde maatregelen periodiek de effectiviteit, ondermeer aan de hand van (sectorale) kpi's
- Vergelijkt de eigen performance op deze maatregelen met de prestaties van de andere waterschappen en eventueel vergelijkbare organisaties
- Beoordeelt derden (w.o. leveranciers, partners, samenwerkingsverbanden) op de effectiviteit van maatregelen, voor zover maatregelen door derden worden uitgevoerd



Beoordelingscriteria, pdca-cyclus

- Verbetert voortdurend de effectiviteit van de maatregelen om de PDCA-cyclus te sluiten



De organisatie doorloopt aantoonbaar en periodiek alle bovengenoemde stappen (werking)

Beoordelingscriteria, organisatie-inrichting, lijn

De bestuurder:

- Is zich bewust van het dreigingsbeeld en de potentiële impact op de maatschappelijke opgave van de organisatie, borgt de beschikbaarheid van de benodigde middelen, overtuigt zich van de effectiviteit en geeft een in-controlverklaring af

De directie:

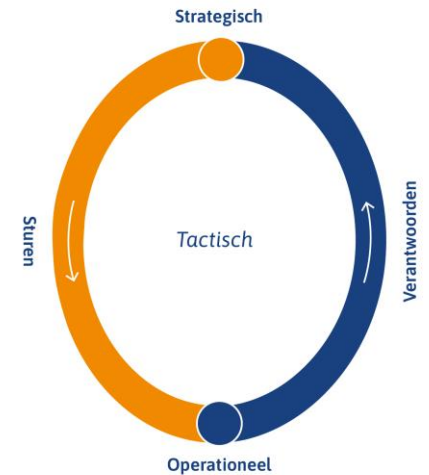
- Toont eigenaarschap van de risico's en de verklaring van toepasselijkheid, ziet toe op het behalen van het beoogde volwassenheidsniveau

Het lijnmanagement:

- Toont eigenaarschap van de maatregelen en ziet toe op uitvoering, meet de effectiviteit en stuurt bij waar nodig

De operatie:

- Voert maatregelen uit, draagt actief bij aan het verbeteren van de effectiviteit en is alert op veiligheids- en privacy-issues



Beoordelingscriteria, organisatieinrichting, staf

De ISO's, OSO's, privacy officers:

- Adviseren, faciliteren, voeren ondersteunende ib- en privacytaken uit (geen eigenaar)

De FG, CISO:

- Onafhankelijk, zonder operationele betrokkenheid of verantwoordelijkheid
- Adviseert over de juiste toepassing van de baselines en organisatie-inrichting
- Helpt de organisatie bij het maken van afgewogen strategische keuzes
- Controleert de werking van de risicoanalyse en de pdca-cyclus en adviseert over verbeteringen
- Heeft een directe lijn naar de bestuurder

Concerncontrol:

- Neemt de thema's mee in de integrale planning- en controlcyclus van de organisatie
- Benoemt de thema's in audits en onderzoeken



Wat heeft de organisatie minimaal nodig

- Een bestuur dat het maatschappelijk belang van de thema's onderkent en vertaalt naar een opdracht voor de organisatie
- Een directie die het belang van informatieveiligheid en privacy in houding en gedrag stimuleert
- Management dat in-control is op deze thema's en stuurt op kwaliteitsmeting en verbetering
- Op de thema's competente en bewuste medewerkers in de processen
- Een IB- en privacy-organisatie die als facilitator op deze thema's fungeert
- Een onafhankelijk gepositioneerde en acterende FG en CISO
- Informatieveiligheid en privacybescherming als onderdeel van de cultuur en de werking van de organisatie
- Werk aan organisatiebreed kwaliteitsmanagement dat het proces van risicomanagement en de PDCA-cyclus ondersteunt



De kracht van samen