Ref. Nr.	Vraag	Antwoord
67	In paragraaf 4.6.2 van de aanbestedingsleidraad en de beantwoording in de nota van inlichtingen wordt gesteld dat voor kerncompetentie 3 (PA) ervaring moet zijn opgedaan “binnen één aaneengesloten periode van 24 maanden bij tenminste vier organisaties”. In de nota van inlichtingen antwoord u dat de beschreven ervaring essentieel is om aan te tonen dat inschrijver voldoende geschikt is. Uw uitvraag richt zich op het auditen van het managementsysteem. Kunt u nader duiden welke auditervaring u in de referenties wilt zien?	Om een managementsysteem te kunnen beoordelen is kennis van het betreffende technisch domein essentieel. Wij verwachten ervaring met het beoordelen van managementsystemen en maatregelensets gericht op procesautomatisering.
68	In paragraaf 4.6.2 van de aanbestedingsleidraad en de beantwoording in de nota van inlichtingen wordt gesteld dat voor kerncompetentie 3 (PA) ervaring moet zijn opgedaan “binnen één aaneengesloten periode van 24 maanden bij tenminste vier organisaties”. In de nota van inlichtingen antwoord u dat de beschreven ervaring essentieel is om aan te tonen dat inschrijver voldoende geschikt is. Uw uitvraag richt zich op het auditen van het managementsysteem. Voor kerncompetenties 1 en 2 die ook gericht zijn op het auditen van het managementsysteem vereist u slechts 1 referentie. Kunt u nader toelichten waarom u het auditen van het managementsysteem voor kerncompetentie 3 belangrijker acht?	Wij brengen geen hiërarchie aan, echter is procesautomatisering essentieel voor de primaire taken van de waterschappen. Vandaar dit onderscheid. Wij zoeken expliciet een leverancier die zich juist op dit domein bewezen heeft
69	In vraag 23 antwoord u dat de volwassenheid dient te worden uitgesplitst naar KA, PA en privacy. In vraag 25 antwoord u dat deelnemers over zowel gecombineerde als gescheiden managementsystemen (en -processen) kunnen beschikken. Kunt u nader toelichten hoe u deze uitsplitsing verwacht wanneer managementsystemen (en -processen) gecombineerd zijn en daarmee de afgrenzing tussen KA, PA en privacy mogelijk vervaagd?	Als een waterschap één integraal ISMS/PIMS heeft , kan dat leiden tot drie gelijke scores. Belangrijk daarbij is dat de rapportage qua opzet aansluit bij de inrichting van het ISMS/PIMS van de organisatie.
70	In uw antwoord op vraag 7 en in de conceptovereenkomst artikel 9.2 en 9.4 vraagt u om het borgen van de inzet van hetzelfde auditteam voor alle 3 de auditrondes. Wij begrijpen uw behoefte en vraag om continuïteit in het auditteam, echter gelet op de gevraagde inspanning (24 audits) in een begrensde periode voor uitvoer (september – december) over een lang uitgerekte periode (3 auditrondes) achten wij de vereisten niet proportioneel. Bent u bereid deze vereiste te beperken tot het kernteam van lead auditor en auditmanagers en daarmee inschrijvers flexibiliteit te bieden, wanneer dit kernteam de continuïteit van de Auditbril borgt?	Wij begrijpen dat u niet de continuïteit van het gehele team voor de duur van de overeenkomst kunt garanderen. Het is aan inschrijver / Opdrachtnemer om dit tussen de verschillende auditcycli zo goed mogelijk te borgen.
71	U geeft aan dat op volwassenheidsniveau 4 de aanwezigheid van een ISMS/PIMS wordt verwacht. Heeft u een indicatie van het aantal deelnemers dat verondersteld op volwassenheidsniveau 4 zit?	In de vorige ronde (2023) was er één waterschap op niveau 4 en een aantal die sterk in die richting gegroeid waren.

Ref. Nr.	Vraag	Antwoord
72	In uw antwoord op vraag 10 geeft u aan niet akkoord te kunnen gaan met ons voorstel inzake de aansprakelijkheidsbeperking. Wij willen u verzoeken dit standpunt te heroverwegen, mede gelet op de disproportionele risicoverdeling die voortvloeit uit de toepassing van de eerste staffel. Zoals eerder toegelicht, leidt de eerste staffel ertoe dat wij als opdrachtnemer mogelijk een aansprakelijkheidsrisico dienen te accepteren dat aanzienlijk hoger ligt dan hetgeen gebruikelijk is binnen onze branche voor vergelijkbare dienstverlening. Ter illustratie: indien het honorarium per audit €20.000 bedraagt, resulteert dit in een aansprakelijkheidslimiet van €150.000 per gebeurtenis. Dit komt neer op een aansprakelijkheid van 7,5 keer het honorarium van een audit, hetgeen niet in lijn is met de uitgangspunten van de AWVODI-2018, waarin een beperking tot drie keer het honorarium wordt beoogd. Wij stellen daarom wij voor om artikel 19.3 van de AWVODI-2018 alsnog aan te passen. In dit geval zijn wij bereid de aansprakelijkheid te verruimen tot vier keer het honorarium voor de werkzaamheden waarin de oorzaak van de schade is gelegen. Wij achten dit voorstel passend en in lijn met de beginselen van proportionaliteit en redelijkheid. Gaat u akkoord met de volgende tekst ter vervanging van de aansprakelijkheidsbeperking uit artikel 19.3 AWVODI-2018: ”De Partij die toerekenbaar tekortschiet in de nakoming van haar verplichtingen, is tegenover de andere Partij aansprakelijk voor de door de andere Partij geleden dan wel te lijden schade. De voornoemde aansprakelijkheid van Opdrachtnemer is beperkt tot een maximum van vier (4) maal het bedrag van het honorarium, dat door Opdrachtnemer aan Opdrachtgever in rekening is gebracht voor het verrichten van de Werkzaamheden waarin de oorzaak van de schade is gelegen, waarbij alleen het honorarium in aanmerking wordt genomen dat betrekking heeft op de laatste twaalf (12) maanden waarin die Werkzaamheden zijn verricht. Het aantal gebeurtenissen is beperkt tot vijf gebeurtenissen en samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.De aansprakelijkheid vervalt na verloop van de wettelijke verjaringstermijn ex. Artikel 3:310 BW. De beperking van de aansprakelijkheid als hiervoor bedoeld is niet van toepassing indien: a. ingeval van aanspraken van derden op schadevergoeding ten gevolge van dood of letsel; b. indien sprake is van opzet of grove schuld aan de zijde van de andere Partij of diens Personeel; c. in geval van schending van intellectuele eigendomsrechten als bedoeld in artikel 22.3 van de Inkoopvoorwaarden.”	Neen, het gevraagde wordt niet overgenomen. Zoals reeds aangegeven in het antwoord op vraag 10 zijn de artikelen van de AWVODI-2018 door de Nederlandse waterschappen gezamenlijk vastgesteld en zijn met inachtneming van enkele evolutionaire wijzigingen ten opzichte van voorgaande versies veelvuldig toegepast en gebruikelijk in de markt. Daarbij valt niet in te zien waarom hier zonder goede grond (bijvoorbeeld in het licht van een specifieke contractuele context, bijvoorbeeld een bijzonder hoog risico) van zou dienen te worden afgeweken. De limitering zoals in de AWVODI opgenomen komt volgens de toelichting ruwweg neer op 3 maal de opdrachtwaarde, maar met een ondergrens van € 150.000 zoals in de AWVODI is bepaald.
73	Wij begrijpen uw wens op de hoogte te zijn van een incident in voorkomend geval. Uiteraard zullen wij, indien dit is toegestaan, een incident bij u melden, alvorens wij – indien noodzakelijk – de Autoriteit Persoonsgegevens en de betrokkenen daarvan op de hoogte brengen. Wij achten het echter redelijk dat wij een redelijke termijn krijgen dit te melden. Daarom stellen wij voor wat betreft de termijn aan te sluiten bij de wettelijke termijn waarbinnen een incident bij de Autoriteit Persoonsgegevens moet worden gemeld, namelijk binnen 72 uur. Kunt u hiermee instemmen?	Als er iets aan de hand is met (persoons-)gegevens van één of meerdere deelnemers, willen wij dat zo snel mogelijk weten.
74	In uw antwoord op vraag 13 staat een verwijzing naar de AWBIT2018. Wij denken dat u abusievelijk deze verwijzing heeft opgenomen in uw antwoord. Kunt u bevestigen dat de AWBIT-2018 niet van toepassing is op deze aanbesteding?	Inderdaad, zoals uit de Overeenkomst blijkt zijn de AWVODI-2018 van toepassing en niet de AWBIT. De term AWBIT-2018 is per abuis in het antwoord op vraag 13 geslopen.

Ref. Nr.	Vraag	Antwoord
75	1. Waar lopen de waterschappen in de praktijk het meest tegenaan bij het beheersen van privacyrisico's / cyber security risico's? 2. Bestaan centrale trainingen en bewustwordingscampagnes binnen de waterschappen op gebied van Privacy en Security en hoe evalueert u zelf de kennis op deze gebieden binnen de waterschappen? 3. Hoe meten de waterschappen of privacy & security maatregelen echt werken? Worden resultaten gedeeld en besproken? 4. Hoe houden de waterschappen overzicht op alle verwerkingen van persoonsgegevens binnen de organisaties, is er per waterschap bijvoorbeeld een actueel register van gegevensverwerkingen? 5. Hoe borgen de waterschappen privacy en security bij samenwerking met externe partijen en leveranciers? 6. Leren de waterschappen actief van andere waterschappen op security en privacygebied? Is er een best practice die is overgenomen? 7. Stel: een nieuwe collega vraagt morgen hoe privacy & security hier goed geregeld is. Wat laten de waterschappen als eerste zien? 8. Hoe wordt privacy en informatieveiligheid in de praktijk besproken, bijvoorbeeld in teamoverleggen?	Al deze vragen zijn inhoudelijke vragen over de wijze waarop waterschappen IV&P binnen de organisatie geborgd hebben. Dat is nu juist het onderwerp van de onderhavige opdracht.
76	U noemt: "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" Gezien de omvang van IEC62443 hierbij volgende vragen ter bespreking:Bestaat er vanuit het Waterschapshuis een concretisering/vertaling wat de volwassenheidsniveaus betekenen voor de PA-omgevingen / IEC62443?	Volwassenheid komt vooral tot uiting in de implementatie van het managementsysteem en de beleving in de organisatie. Zie ook de illustratie hiervan (3 lagen plaat) in de presentatie van de per-bid meeting op 11 september. Dat staat los van de maatregelen in IEC62443.
77	Is er een tijdslijn waarbinnen het Waterschapshuis verwacht dat de waterschappen binnen hun PA-omgevingen welk niveau halen?	Nee.
78	Is er een tijdslijn waarbinnen het Waterschapshuis verwacht dat de waterschappen binnen hun PA-omgevingen voldoen aan de cyberbeveiligingswet (NIS2) en CER?	Nee.
79	Verwacht u binnen het assessment van de PA-omgeving dat wij ook technische steekproeven uitvoeren binnen systemen in de (decentrale) PA-omgevingen?	Nee.
80	Wat zijn de belangrijkste lessen uit de vorige meetingen?	Twee belangrijke lessen: 1. Dat de planning strak wordt nageleefd 2. Dat opdrachtnemer zorgt voor een constante auditbril niet allleen binnen een auditcyclus, maar ook tussen de opvolgende auditcycli.
81	Vanaf 24 september 2025 tot de inwerkingtreding van de Cbw hanteren de provincies, waterschappen en het Rijk de BIO2 als verplichtende zelfregulering. Ziet u hiermee in de audits ook een belang om te rapporteren over aan welke zaken uit het ISMS conform BIO2 een Deelnemer nog niet voldoet naast het rapporteren over het volwassenheidsniveau?	Jazeker. BIO2 is voor de waterschappen leidend en moet worden toegepast.
82	Mogen wij ervan uitgaan dat alle Deelnemers dezelfde reikwijdte van het ISMS (managementsysteem) hebben? Immers, BIO2 biedt de mogelijkheid voor een organisatie om minimaal de bedrijfsprocessen en informatiesystemen op te nemen die kritisch zijn voor haar dienstverlening in plaats van de volledige organisatie.	Nee. Scopebepaling is aan de waterschappen zelf.

Ref. Nr.	Vraag	Antwoord
83	De vastgestelde BIO2 kent een self-assessment vragenlijst (BIO-SA) op basis van het CIP BIO Volwassenheidsmodel met vijf (5) niveaus. Is de vaststelling van BIO2 inclusief de genoemde verplichtende zelfregulering aanleiding voor Opdrachtgever om het tot nu toe gehanteerde volwassenheidsmodel van Opdrachtgever met BIO-SA en het CIP-model in lijn te brengen? Indien Opdrachtgever het huidige volwassenheidsmodel wenst te blijven hanteren, kan Opdrachtgever dan bevestigen dat Opdrachtnemer in rapportages (individueel dan wel sectoraal) geen aandacht hoeft te besteden aan de scores zoals deze zouden volgen uit BIO-SA en het CIP-model (bijvoorbeeld door een omzettingstabel)?	Voor zover ons bekend is de CIP BIO-SA nog niet aangepast op BIO2. Daarnaast ligt in de BIO-SA het accent sterk op maatregelen, waar in de voorliggende opdracht de focus op het managementsysteem ligt. Vooralsnog zullen wij ons eigen volwasseneheidsmodel hanteren.
84	U schrijft 'wij bedoelen met "een actieve rol" dat de lead-auditor actief participeert in de uitvoering van de audits'. Verwacht Opdrachtgever hiermee dat de lead-auditor zichtbaar aanwezig is bij tenminste één (1) interviewronde op locatie bij alle Deelnemers? Of kan de lead-auditor deze actieve rol bijvoorbeeld ook invullen door zichtbaar alle voorlopige resultaten te reviewen en betrokken te zijn bij het opstellen van alle conceptrapporten?	Hoe u de zichtbaarheid van de lead-auditor uitwerkt in uw aanpak is aan u en zal meewegen in onze beoordeling van de inschrijving. Waar wij in de stukken spreken over "de lead-auditor" mag ook "de lead-auditors" worden gelezen.
85	In de aanbestedingsleidraad 5.1.3 benoemt u maximaal zes (6) verschillende typen in te zetten functionarissen. In de NvI 1 benoemt u dat voor elke deelnemer van het aangeboden auditteam een CV overlegd dient te worden. Is onze aanname juist dat wanneer wij per type functionaris over meerdere geschikte en inzetbare auditoren beschikken wij al deze CV's geanonimiseerd vooraf dienen in te dienen? Of dienen wij te lezen dat het totale auditteam uit maximaal 6 vaststaande auditoren (inclusief lead-auditor) dient te bestaan?	U levert per type functionarissen alle CV's van de door u in te zetten personen in.
86	Wat zijn voor u criteria met betrekking tot 'naarmate het bemensingsplan meer weet te overtuigen' zoals geformuleerd in de aanbestedingsleidraad (5.1.3)? Hebt u als Opdrachtgever impliciete dan wel expliciete verwachtingen bij 'reële urenaantallen en reële uurtarieven' aangezien u deze begrippen hebt opgenomen in de aanbestedingsleidraad?	Daar hebben wij geen expliciete verwachtingen bij, echter de vaste prijs geeft u richting op de in te zetten capaciteit.
87	Vorige vraag) Hoe zien jullie het verschil tussen de volwassenheidsmeting van het laboratorium en het waterschapshuis zelf in verhouding tot de waterschappen?	hWh en de Unie van Waterschappen hebben geen PA. Het lab heeft heel specifieke PA, namelijk de laboratoriumsoftware. Voor alle organisaties geld echter het beoogde volwassenheidsniveau. Context is anders, het ISMS zal echter dezelfde elementen moeten bevatten.
88	Is het nog zinvol om hWh als eerste Deelnemer te auditen?	Nee, daar is geen noodzaak voor.
89	Zijn de vorige metingen die zijn uitgevoerd ook op volwassenheidsniveau uitgevoerd? En zo ja kan HWH een indicatie geven van de volwassenheidsscore / benchmark uit die meting?	Er was één organisatie die 4 of hoger scoorde. Een aantal waterschappen zaten tussen 3,5 en 4 en de grote middenmoot tussen 2,8 en 3,5. En een enkele achterblijver.
90	Op basis van welke normen, standaarden en referentie? Dit om zoveel mogelijk appels met appels te vergelijk ook in de groei.	Vorige rapportages volgen de de structuur van CIP. Dit laten we nu los, we maken de stap naar ISO. We zijn niet op zoek naar rapportages volgens het specifieke framework van Opdrachtnemer, maar meer naar open rapportagestructuren, bijvoorbeeld zoals het recent gelanceerde Cbw (NIS2) Framework van NOREA/Auditdienst Rijk.
91	Effectiviteit van verbeteringen n.a.v. deze metingen zijn wel onderdeel van de scope?	Ja, in lijn met hoofdstuk 10 ISO.
92	Er wordt gesproken binnen het waterschapshuis over CIP framework moet dit ook worden meegenomen?	Nee. Het CIP-raamwerk is gebruikt voor maatregelen in de vorige audits. Toetsing van maatregelen is echter buiten scope van deze opdracht.
93	Rapportages volgens de hoofdstukken van ISO 27001 hoe verhoudt dit zicht tot hoofdstuk 5 ISO 27701 (moet dit apart of worden geïntegreerd?)	ISO27701 verwijst in hoofdstuk 5 naar hoofdstuk 4 tot en met 10 van ISO27001. Rapportages kennen de structuur van ISO27001, ook voor privacy.

Ref. Nr.	Vraag	Antwoord
94	Huidige CSIR is gebaeerd op BIO1. Hoe zien jullie ontwikkelingen op het gebied van CSIR.	CSIR is een implemenatierichtlijn, vooral gericht op maatregelen. Verwachting is dat CSIR aangepast wordt aan de BIO2. CSIR is een best-practice implementatierichtlijn, net als ISO27002, en toetsing van maatregelen valt buiten scope van de opdracht.
95	Term Audit? Hoe moeten we die uitleggen?	De term Audit moet niet gelezen worden als een ja/nee vraag en is niet gericht op compliance of assurance. De bedoeling is het beantwoorden van de volwassenheidsvraag. De meting is uitdrukkelijk gericht op leren en verbeteren.
96	Planning: kunnen we flexibel omgaan met de planning?	De doorlooptijden binnen een audit zijn in beginsel vast. Dat betekent niet dat er niet dat zich niet incidenteel een uitzonderlijke situatie kan voordoen, waarin gemotiveerd moet worden afgeweken. Een herhaald patroon is niet aanvaardbaar. Tijdige en transparante communicatie over een incidentele vertraging is in zo'n geval wel een vereist.
97	Prepared by client (PBC) lijst. Welke voorbereiding kunnen we verwachten van de deelnemers?	Dat is met name aan opdrachtnemer om daar structuur in te geven en met Deelnemers afspraken over te maken.
98	Verwacht u dat wij een lead-auditor inzetten of mogen we ook meerdere lead-auditors inzetten voor deels overlappende audits bij de verschillende waterschappen ?	U bent zonder meer vrij om meerdere lead-auditors in te zetten bij de uitvoering van de werkzaamheden.
99	Op pagina 14 wordt bij kerncompetentie 2 gevraagd om “ervaring om audits op het gebied van privacy in een organisatie met tenminste 500 medewerkers”. Klopt het dat hier niet specifiek wordt gevraagd om een audit op het PIMS, maar een privacy audit in brede zin. Zou bijvoorbeeld een audit op privacy maatregelen ook invulling geven aan het gevraagde?	Inderdaad er wordt niet specifiek gevraagd om een audit op het PIMS. Een audit op privacy maatregelen zou, als is voldaan aan alle vereisten van de kerncompetentie, ook kunnen volstaan.
100	Op pagina 14 wordt bij kerncompetentie 3 gevraagd om ervaring met “audits op het gebied van informatieveiligheid van procesautomatisering waarbij de procesautomatisering wordt gebruikt voor het beheer van operationele processen in de fysieke wereld voor het aansturen en monitoren van industriële apparatuur en/of infrastructuur”. Klopt het dat hier niet specifiek wordt gevraagd om een audit op het ISMS, maar een audit op “informatieveiligheid van procesautomatisering waarbij de procesautomatisering wordt gebruikt voor het beheer van operationele processen in de fysieke wereld voor het aansturen en monitoren van industriële apparatuur en/of infrastructuur” in brede zin. Zou bijvoorbeeld een audit op de genomen maatregelen ook invulling geven aan het gevraagde?	Inderdaad er wordt niet specifiek gevraagd om een audit op het ISMS. Een audit op de genoemen maatregelen zou, als is voldaan aan alle vereisten van de kerncompetentie, ook kunnen volstaan.
101	Op pagina 14 en 15 wordt bij de referenties gevraagd om uitvoering op regelmatige wijze van de opdrachten. Hoe kunnen wij het “op regelmatige wijze” uitvoeren interpreteren wanneer het gaat om het aanleveren van 1 referentie?	Op “vakkundige en regelmatige wijze" wil zeggen dat de opdracht professioneel, deskundig en naar behoren is uitgevoerd. Dit impliceert een zorgvuldige, correcte en volgens de in de branche geldende normen uitvoering van de opdracht.
102	In formulier 3 Referentieprojecten kerncompetentie wordt gevraagd om gegevens van een contactpersoon van de opdrachtgever. Ondanks dat opdrachtnemer hierover beschikt is het voor opdrachtgever enkel relevant dat de referentie van de winnende inschrijver verifieerbaar is. Is opdrachtgever bereid om, in het kader van het verlagen van de inschrijvingslast, het ontvangen van de contactgegevens te beperken tot de winnende inschrijver?	Neen, het gevraagde wordt niet overgenomen. hWh moet rechtstreeks contact kunnen opnemen met referenties zonder uw tussenkomst.
103	Moet een referentie betrekking hebben op een assurance opdracht?	Neen, in de eis van de kerncompetenties wordt niet verlangd dat een referentieopdracht betrekking heeft op een assurance opdracht.

Ref. Nr.	Vraag	Antwoord
104	Op pagina 18 van de Aanbestedingsleidraad staat omschreven dat de inschrijver bij zijn inschrijving een uitleg moet geven die getuigt van adequate organisatiesensitiviteit. Daarbij wordt als doelstelling genoemd dat de opdrachtnemer bij de uitvoering van de opdracht bewust moet zijn van de verschillen in de lagen van een organisatie en een passende gesprekspartner moet zijn voor de verschillende typen functionarissen. Daarnaast staat op pagina 6 van dezelfde leidraad dat (i) de opdrachtnemer die de waterschapssector en -cultuur goed kan inschatten en met een bijpassende bestuurlijke sensitiviteit haar rapportages opstelt en dat (ii) de waterschappen individuele en onafhankelijke organisaties zijn met eigen besturen en invulling van doestellingen en dat opdrachtnemer gepast dient om te kunnen gaan met diverse organisatietypen en culturen en zich kan inleven in de doestelling van de audits. Ligt het zwaartepunt van het vereiste organisatiesensitiviteit op één niveau (sectoraal, waterschappen onderling, dan wel organisatielagen binnen een organisatie) of dienen deze verschillende niveaus alle drie in gelijke mate terug te komen in de inschrijving en de uitvoering van de opdracht?	Organisatiesensitiviteit speelt in alle lagen van de organisatie en kan in verschillende lagen een verschillende benadering met zich meebrengen.
105	Eis 1.1 geeft aan dat "Het toetsen van maatregelen behoort niet tot de scope." De afgesproken scope richt zich nu op ISMS voor KA, PA en privacy. Waarom worden de beheersmaatregelen buiten scope gehouden?	Het toetsen van beheersmaatregelen is onderwerp van eerdere toetsingen geweest. Nu ligt de focus op het managementsysteem. Dit is een keuze van de sector.
106	De BIO2 gebaseerd op ISO27001 en 2 en bevat ook beheersmaatregelen voor bijvoorbeeld fysieke beveiliging, leveranciersmanagement en continuiteitsbeheer. Hoewel deze nu buiten de formele scope zijn geplaatst, vereist een ISO en/of BIO2 audit wel dat we hier zicht op hebben. Hoe wil hWh dat we hiermee omgaan: strikt uitsluiten, signaleren als aandachtspunt, of indicatief meenemen?	U onderzoekt het managementsysteem, waaronder de verklaring van toepasselijkheid. Aan de hand hiervan staat het u vrij om te onderzoeken of maatregelen waarvan de organisatie zegt ze geïmplementeerd te hebben, te toetsen op juistheid. Het beoordelen van de (opzet, bestaan en werking van de) maatregelen is geen onderdeel van de opdracht.
107	Heeft hWh ook de intentie om de audit scope te verbreden naar de andere kritische business processen en de beheersmaatregelen op lange termijn?	Er is geen intentie om de scope te verbreden.
108	Hoe zien jullie de toekomst van de resulaten van audits?	Alle Deelnemers zijn zelfstandig en maken hun eigen afwegingen. De resultaten bevatten niet alleen aanbevelingen voor verbeteringen op Deelnemers niveau, maar ook wordt een sectoraal rapport verlangd met aanbevelingen voor voor verbeteringen op sectoraal niveau.
109	Kunnen jullie Procesautomatisering nader duiden?	De waterschappen hebben veel installaties en kunstwerken in de fysieke wereld die worden beheerd en bestuurd met systemen voor industriële automatisering. De verschillende waterschappen zijn zelfstandige organisatie en hebben verschillende oplossingen.
110	Kunnen jullie de Kantoorautomatiserings-omgeving duiden?	Met KA bedoelen we alle systemen die in de kantooromgeving worden gebruikt. Denk daarbij aan bijvoorbeeld Microsoft365, ERP-software, zaaksystemen, HRM-systemen, workflowsystemen.
111	Het sectorale volwassenheidsniveau is gemiddeld niveau 3. Wat houdt deze waarde in, in relatie tot de Plan Do Check Act-cycle?	In grote lijnen kan gesteld worden dat niveau 3 betekent dat maatregelen geïmplementeerd zijn of op een implementatieplanning staan. (Plan Do).
112	Wat is de meetlat om tot gemiddeld sectorale volwassenheidniveau van 3 te komen?	In grote lijnen kan gesteld worden dat niveau 3 betekent dat maatregelen geïmplementeerd zijn of op een implementatieplanning staan.
113	Wat zijn de outlayers ten aanzien van het sectorale systeem?	Er was één organisatie die 4 of hoger scoorde. Een aantal waterschappen zaten tussen 3,5 en 4 en de grote middenmoot tussen 2,8 en 3,5. En een enkele achterblijver.
114	Wat is de meetlat om tot gemiddeld sectorale volwassenheidniveau van 3 te komen?	In grote lijnen kan gesteld worden dat niveau 3 betekent dat maatregelen geïmplementeerd zijn of op een implementatieplanning staan.

Ref. Nr.	Vraag	Antwoord
115	Wat zijn de outlayers ten aanzien van het sectorale systeem?	Er was één organisatie die 4 of hoger scoorde. Een aantal waterschappen zaten tussen 3,5 en 4 en de grote middenmoot tussen 2,8 en 3,5. En een enkele achterblijver.
116	De BIO 2.0 komt eraan. In hoeverre willen jullie deze meenemen in de audit eind 2026?	De BIO2 is inmiddels gepubliceerd en moet worden meegenomen.
117	Ik begrijp dat het Waterschapshuis een kritisch opbouwend adviesrapport wil ontvangen. Dit betekent vanuit mijn standpunt, dat wij zullen aangeven wat goed of minder goed gaat. Voor het goede geven wij aan waarom dit goed gaat en voor de minder goede aspect zullen wij een advies verstrekken. Ligt dit in de lijn van de verwachting?	Het rapport mag kritisch zijn als daar aanleiding voor is, maar het rapport moet wel motiveren tot verbetering.
118	1. U vraagt onder meer aan een auditor een adviesrapport. Begrijpt u, op welke wijze wij deze opdracht in een (advies) rapport moeten gieten?	We zoeken uitdrukkelijk geen assurancerapport. We zoeken wel een adviesrapport waarin we leren wat we moeten doen om te groeien in volwassenheid. Het adviesrapport geeft input aan het leer- en verbetertraject voor de Deelnemers. Binnen de sector willen we ook wel weten welke mogelijkheden er zijn om beter/meer samen te werken (waar liggen kansen die we zelf niet zien), bijv. IT en architectuur. Werkzaamheden tussen waterschappen verschillen (een enkel waterschap beheert ook wegen, sommige hebben ook een eigen laboratorium of belastingkantoor en een waterschap is (nu nog) gecombineerd met een drinkwaterbedrijf (scope daarvan is alleen het waterschapsbedrijf dat naar verwachting per 1 januari 2026 is afgescheiden).
119	Verantwoordelijkheid informatiebeveiliging ligt bij de waterschappen. Is bij elk waterschap een CISO?	BIO geeft daar richtlijnen voor: bestuur is eindverantwoordelijk, directie is verantwoordelijk voor implementatie maar hoe dat verschilt per waterschap. Overal is wel een CISO en FG maar de inbedding varieert.