Bijlage E - Programma van eisen

Behoort bij de Overeenkomst Audits BIO & AVG, kenmerk Z1837.

Eisen 1. Inhoudelijke eisen	
Eis 1.1	De audit heeft de vorm van een systeemgerichte toetsing van opzet, bestaan én werking van het managementsysteem voor informatieveiligheid KA, informatieveiligheid PA en privacy conform ISO27001 en ISO27701 (hoofdstuk 5) bij de Deelnemers. Het toetsen van maatregelen behoort niet tot de scope. De audit is niet gericht op het rapporteren van afwijkingen, maar gericht op het krijgen van aanbevelingen voor verbetering. Toelichting: er kan bij een Deelnemer sprake zijn van een informeel proces waarbij opzet en/of bestaan niet of minder aanwezig zijn. Dit laat het toetsen van de (informele) werking onverlet.
Eis 1.2	Opdrachtnemer dient bij elke individuele Deelnemer de opzet, het bestaan én de werking te toetsen van het managementsysteem voor informatieveiligheid KA, informatieveiligheid PA en privacy, met als norm BIO2 en AVG; onderliggend ISO27001 en ISO27701 (Hoofdstuk 5), inhoudende: • instrumentele toetsing van de betreffende processen en producten op basis van door de waterschappen aan te leveren documentatie; • bespreking documentatie tussen auditor en de organisatie; • interviews houden met sleutelfunctionarissen om het niveau van volwassenheid vast te stellen op basis van de sectorale uitwerking van volwassenheidsniveau 4*, resulterend in een kwalitatief oordeel over het managementsysteem (ISMS/PIMS) met concrete en praktisch toepasbare aanbevelingen voor verbetering en verdere groei in volwassenheid. * *zie bijlage F – Uitwerking volwassenheidsniveau 4 in de waterschapssector, versie 1.02 van september 2023 of in geval van actualisatie, de geactualiseerd versie.*
Eis 1.3	De lead-auditor van een auditteam is geregistreerd in het NOREA register of CISA gecertificeerd in het ISACA register.

hetWaterschapshuis | Stationsplein 89 3818 LE Amersfoort | Postbus 2180 3800 CD Amersfoort | T 033 460 31 00
info@hetwaterschapshuis.nl | www.hetwaterschapshuis.nl | IBAN NL25NWAB0636756262 | BIC NWABNL2G | KvK-nummer 56683464

Eis 1.4	Interviews met sleutelfunctionarissen vinden plaats op locatie bij de Deelnemer. Online sessies zijn niet toegestaan. Sleutelfunctionarissen voor de interviews bevinden zich in de doelgroepen: • Directie; • Lijnmanagement direct onder directieniveau; • Teamleiders en medewerkers; • Domeinspecialisten Risk, IB en privacy.
Eis 1.5	De resultaten van de audits tussen de Deelnemers onderling moeten vergelijkbaar zijn. Dit betekent dat dezelfde Auditbril dient te worden gehanteerd. De audits hebben niet als doel een onderlinge ranking van waterschappen.
Eis 1.6	Opdrachtnemer beoordeelt in welke mate de in voorgaande externe sectorale audit gedane aanbevelingen aan Deelnemer zijn opgevolgd.
Eis 1.7	Opdrachtnemer toont een proactieve en ontzorgende houding naar Deelnemers en Opdrachtgever.
Eis 1.8	Opdrachtnemer is zelf verantwoordelijk voor de coördinatie en planning van de audit.
Eis 1.9	Opdrachtnemer zorgt voor een beveiligde en gebruiksvriendelijke digitale omgeving waar Deelnemers hun documentatie kunnen aanleveren. Opdrachtnemer draagt zorg voor een passend niveau van beveiliging naar de huidige stand van techniek van deze omgeving en ziet toe op instandhouding daarvan.
Eis 1.10	Opdrachtnemer zorgt voor de inzet van voldoende vakbekwaam Personeel van Opdrachtnemer bij de uitvoering van de audits.
Eis 1.11	Opdrachtnemer zorgt voor toepassing van dezelfde Auditbril door de verschillende auditteams.
Eis 1.12	De voertaal voor de audits en rapportages in woord en geschrift is Nederlands.
Planning	
Eis 1.13	Planning van de auditcyclus: 1. Februari 2026: opstart operationeel team Opdrachtgever en Opdrachtnemer, briefing en kennismaking met auditteams Opdrachtnemer. 2. Half april: eerste presentatie auditaanpak, voorbereiding en tijdspad aan de Deelnemers.

	3. Begin juni: tweede presentatie voorbereidingen, te verzamelen ondersteund bewijs, oproep tot intekenen op tijdblok. 4. Begin juli: planning waterschappen bekendgemaakt, aanleverportaal gereed. 5. Op zijn laatst 1 september: start audits. 6. 1 oktober: toets op eerste conceptrapportages door hWh op inhoud/tone-of-voice. 7. 1 december: audits gereed, conceptrapporten bij de laatste waterschappen. 8. 15 december: definitieve eindrapporten bij alle waterschappen. 9. 31 januari 2027: sectorrapport gereed, debriefing, evaluatie. 10. Februari t/m april 2027: gelegenheid voor presenteren auditresultaten in diverse gremia, houd rekening met 4 presentaties op nader te bepalen locatie. Deze planning is mutatis mutandis van toepassing voor de tweede (2029-2030) en derde auditcyclus (2032-2033).
Eis 1.14	De doorlooptijd voor een audit bij een Deelnemer is 8 weken. Tijdspad audit Deelnemer: 1. Begin week 1: intakegesprek, kennismaking, laatste vragen over te verzamelen ondersteunend bewijs. 2. Eind week 2: ondersteunend bewijs door waterschap aangeleverd bij auditpartij. 3. Week 4: audit managementsysteem IB/Privacy, interviews volwassenheid. 4. Begin week 6: conceptrapportage bij Deelnemer. 5. Eind week 7: feedback/verificatiegesprek met auditor (let op: 1 ronde feedback). 6. Eind week 8: definitief rapport bij Deelnemer. Afwijken van deze planning is alleen toegestaan na akkoord van de deelnemende organisatie en de projectleider van hWh. Opdrachtnemer, Deelnemer en projectleider van hWh leggen bindende afspraken vast over de gewijzigde planning.

Eisen 2. Rapportage resultaten	
Eis 2.1	Rapportages worden in afstemming met de projectleider van hWh op een beveiligde manier gedeeld met de Deelnemer(s), respectievelijk Opdrachtgever.
Eis 2.2	Voor de rapportages hanteert Opdrachtnemer een gestandaardiseerd format. Opdrachtnemer legt het format voor aanvang van de toetsing voor aan hWh ter beoordeling van de juistheid en toepasbaarheid ervan. Opdrachtnemer past het format toe met inachtneming van de feedback van hWh.
Eis 2.3	**1**. Opdrachtnemer dient, zodra de eindrapportages van de eerste drie Deelnemers gereed zijn, deze voor te leggen en te bespreken met de Projectgroep Audits. Aan de hand van deze praktijkvoorbeelden wordt een gezamenlijk beeld gevormd van de kwaliteit van de rapportages, met als doel om – waar nodig - de vorm, formulering en benadering van de rapportages in een zo vroeg stadium bij te kunnen stellen. **2**. Na de evaluatie stelt Opdrachtnemer de overige individuele rapportages op met inachtneming van de uit de evaluatie voortvloeiende wijzigingen.
Rapportage Deelnemer	
Eis 2.4	Opdrachtnemer stelt van elke audit bij een Deelnemer een (individueel) vertrouwelijk auditrapport op.
Eis 2.5	De rapportage bevat geen persoonsgegevens. In de rapportage opgenomen casussen zijn niet herleidbaar naar individuele personen.
Eis 2.6	De auditrapportage bevat organisatie-specifieke bevindingen, daaruit voortvloeiende volwassenheidsscores en concrete, passende en uitvoerbare aanbevelingen voor verbetering voor de individuele Deelnemer.
Eis 2.7	De auditrapportage geeft inzicht in de borging en volwassenheid van de informatiebeveiliging binnen zowel kantoorautomatisering, als procesautomatisering en privacy. De audit ziet toe op een periode van een jaar teruggerekend vanaf de auditdatum.
Eis 2.8	De auditrapportage geeft inzicht in hoe de Deelnemer presteert ten opzichte van de norm, zowel grafisch (spinnenwebgrafiek) als tekstueel. De spinnenwebgrafiek bevat de volgende assen (gebaseerd op ISO27001): • Context • Leiderschap • Planning (Risicomanagement) • Ondersteuning • Uitvoering • Evaluatie van de prestaties • Verbetering

Eis 2.9	De aanbevelingen voor verbetering zijn passend en praktisch toepasbaar in de context van de betreffende Deelnemer en bij de aard en het karakter van de processen van de waterschappen.
Eis 2.10	De auditrapportage wordt in concept voorgelegd aan de contactpersoon van de Deelnemer.
Eis 2.11	De auditrapportage wordt met in achtneming van de feedback van Deelnemer als definitief rapport gericht aan de directie, CISO, FG en het eerste aanspreekpunt voor de audit van de betreffende Deelnemer.
Sectorrapportage	
Eis 2.12	Na afronding van de individuele rapportages aan Deelnemers, stelt Opdrachtnemer een sectorrapport op, alsmede een score-overzicht (tabel) van alle volwassenheidsscores van deelnemende organisaties.
Eis 2.13	Het sectorrapport geeft de sectorale status van de informatieveiligheid KA, informatieveiligheid PA en privacy in de waterschapsector (bestaande uit de waterschappen, het Waterschapshuis en de Unie van Waterschappen)*. *Andere Deelnemers worden niet opgenomen in de sectorrapportage.
Eis 2.14	De informatie in het sectorrapport dient geschikt te zijn voor openbaarmaking en niet herleidbaar naar een individuele Deelnemer.
Eis 2.15	Het sectorrapport bevat een managementsamenvatting waarin onder andere generieke aanbevelingen voor verbetering en volwassenheidsscores worden weergegeven.
Eis 2.16	Het sectorrapport bevat aanbevelingen voor verbetering met prioritering die sectoraal opgepakt kunnen worden.
Eis 2.17	De aanbevelingen voor verbetering zijn concreet, praktisch toepasbaar en bieden handelingsperspectief.
Eis 2.18	De sectorrapportage en score-overzicht wordt in concept voorgelegd aan de projectleider hWh.
Eis 2.19	Het sectorrapport en score-overzicht wordt met in achtneming van de review feedback opgeleverd als definitief sectorrapport aan hWh.
Eis 2.20	Opdrachtnemer presenteert op basis van het sectorrapport in de waterschapsector over de mate van volwassenheid aan de volgende drie doelgroepen: - Secretarissen-Directeur; - i-Beraad; - CISO's en FG's.

Eisen 3. Voortgangsoverleg en -rapportage	
Eis 3.1	Opdrachtnemer houdt Opdrachtgever op de hoogte van de voortgang van de audits middels tweewekelijkse voortgangsoverzichten. Het voortgangsoverleg heeft betrekking op alle aspecten van de uitvoering van de opdracht, waaronder de planning, knelpunten en klachten.
Eis 3.2	Voortgangsoverzichten worden twee werkdagen voor het voortgangsoverleg beschikbaar gesteld aan de projectleider van hWh.
Eis 3.3	De aangewezen contactpersonen van Opdrachtnemer en Opdrachtgever hebben iedere 14 dagen voortgangsoverleg. De frequentie kan worden verhoogd indien de projectleider hWh of Opdrachtnemer daar aanleiding voor ziet.
Eis 3.4	Alle voortgangsoverleg vindt plaats op een door de projectleider hWh te bepalen locatie of in digitale vorm.
Eis 3.5	Voor alle overlegvormen over de voortgang draagt Opdrachtnemer zorg voor de verslaglegging en verstrekt deze binnen 5 werkdagen, in een gangbaar digitaal bestand aan de projecteider hWh.
Eis 3.6	Rapportages dienen transparant opgesteld te worden. Dit houdt in dat: • Voortgang duidelijk te volgen is. • Rapportages een consistente gedragslijn volgen. • Tekortkomingen en aandachtspunten gesignaleerd worden en oplossingen worden benoemd (verbetervoorstellen). Daarnaast dient een rapportage een helder en duidelijke tendens zichtbaar te maken voor wat betreft het oplossen van tekortkomingen en aandachtspunten.
Eis 3.7	De in het voortgangsoverleg afgesproken verbetermaatregelen zijn bindend.
Eis 3.8	Partijen informeren elkaar, zowel tijdens de uitvoering van een auditcyclus als tussen de auditcycli, proactief en tijdig over gebeurtenissen die de voortgang, kwaliteit of continuïteit van de audit en/of een volgende auditcyclus kunnen beïnvloeden.

Eisen 4. Privacy	
Eis 4.1	Opdrachtnemer zal de toegang en de autorisaties die zijn verleend ten behoeve van de uitvoering van de dienst(en) enkel voor dat doeleinde gebruiken en niet voor enig ander doeleinde.
Eis 4.2	Opdrachtnemer meldt binnen 72 uur na ontdekken van datalek aan Opdrachtgever dat er een datalek heeft plaatsgevonden waarbij persoonsgegevens van Opdrachtgever betrokken zijn.
Eis 4.3	Medewerkers van Opdrachtnemer hebben alleen toegang onder geheimhoudingsverplichting. Een geheimhoudingsverplichting als onderdeel van de arbeidsovereenkomst tussen werknemer en opdrachtnemer volstaat hiertoe.
Eis 4.4	Verwerking van (persoons)gegevens van de Opdrachtgever dient alleen binnen de EER plaatsvinden.
Eis 4.5	Opdrachtnemer is zelfstandig verwerkingsverantwoordelijke voor deze opdracht en draagt daarmee een eigen verantwoordelijkheid ter bescherming van de persoonsgegevens die worden verwerkt ten behoeve van de opdracht.
Eis 4.6	(Gearchiveerde) data behoort gedurende de overeengekomen bewaartermijn, technologie-onafhankelijk, raadpleegbaar, onveranderbaar en integer te worden opgeslagen en op aanwijzing van opdrachtgever aantoonbaar te kunnen worden vernietigd.