

Marktconsultatieverslag

Het Waterschapshuis

t.b.v.

Auditdienstverlening t.b.v. Baseline Informatiebeveiliging Overheid (BIO) en Algemene Verordening Gegevensbescherming (AVG)

Versie 1.0

Publicatiedatum: 8 november 2019

Auteur: Stefan de Jong

Ons kenmerk: Z1645/H009241

Colofon

Titel: Marktconsultatieverslag Auditdienstverlening t.b.v. BIO en AVG

Auteur(s): Stefan de Jong

Contactpersoon: Stefan de Jong

Vervangend contactpersoon: John Jonkhout

Het Waterschapshuis, 8 november 2019

Stationsplein 89, 3818 LE Amersfoort

Postbus 2180, 3800 CD Amersfoort

T: 033 460 31 00, F: 033 460 31 01

www.hetwaterschapshuis.nl, inkoop@hetwaterschapshuis.nl

Inhoud

1. Inleiding	2
1.1 Achtergrond marktconsultatie	2
1.2 Doel marktconsultatie	2
2. Vragen	3
Organisatie van het onderzoek	3
2.1 Vraag 1	3
2.2 Vraag 2	4
2.3 Vraag 3	5
2.4 Vraag 4	7
Normenkader	8
2.5 Vraag 1	8
2.6 Vraag 2	8
2.7 Vraag 3	8
2.8 Vraag 4	9
Kwaliteitsborging van het onderzoek	9
2.9 Vraag 1	9
2.10 Vraag 2	10
2.11 Vraag 3	11
Volwassenheidsniveaus	11
2.12 Vraag 1	11
2.13 Vraag 2	12
2.14 Vraag 3	13
Auditcyclus	14
2.15 Vraag 1	14
2.16 Vraag 2	14
2.17 Vraag 3	15
Kosten	16
2.18 Vraag 1	16
2.19 Vraag 2	16

1. Inleiding

Voor u ligt het verslag van de marktconsultatie inzake auditdiensten op de Baseline Informatiebeveiliging Overheid (hierna: BIO) en de Algemene Verordening Gegevensbescherming (hierna: AVG) zoals door het Waterschapshuis (hierna: opdrachtgever) is gehouden in opdracht van 21 waterschappen, de Unie van Waterschappen (hierna: UvW) en Waterschapsbedrijf Limburg (hierna: WBL).

1.1 Achtergrond marktconsultatie

Opdrachtgever is voornemens een aanbesteding in de markt te zetten welke auditdiensten op de BIO en de AVG uitvraagt.

Voor deze marktconsultatie zijn marktpartijen uitgenodigd die mogelijkheden zien eigenhandig te voorzien in de audit-behoefte van opdrachtgever. Binnen de waterschapsector zijn de BIO en de AVG geïntegreerd ingevoerd wegens de grote onderlinge samenhang. Een mogelijke geïntegreerde aanpak vanuit de auditor geniet vanuit opdrachtgever dan ook een zeer sterke voorkeur.

De organisaties, welke opdrachtgever vertegenwoordigt, kennen een grote diversiteit in organisatiecultuur. Daarnaast hebben deze organisaties allen een eigen volwassenheidsniveau en ontwikkelplan. Verwacht wordt dat marktpartijen hier in hun rapportage rekening mee kunnen houden en als direct gevolg hiervan in staat is om de juiste cultuur-sensitiviteit in haar rapportages aan te brengen. Opdrachtgever heeft tot doel de auditresultaten te gebruiken om:

1. Inzicht te verkrijgen in de onderlinge verhoudingen tussen waterschappen;
2. Inzicht te verkrijgen in de status van elke individuele organisatie;
3. Voortgang in organisatievolwassenheid en implementatiekwaliteit van de BIO en AVG vast te leggen;
4. Verbeterinitiatieven per organisatie (of sectorbreed) te initiëren om als waterschapsector naar een hoger volwassenheidsniveau te groeien.

Marktpartij dient aan de individuele deelnemende organisaties verbeterpunten aan te leveren teneinde een vooraf gespecificeerd en afgestemd volwassenheidsniveau in de gehele sector te behalen. Daarnaast dient aan opdrachtgever, per auditperiode, een planmatig geaggregeerde sectorrapportage opgeleverd te worden welke inzicht geeft in kansen op samenwerking binnen de sector ter verbetering van de organisatievolwassenheid binnen de sector. Zowel per individueel waterschap als voor de sector wordt een volwassenheidsniveau bepaald.

1.2 Doel marktconsultatie

Deze consultatie van de markt is uitgevoerd met als hoofddoel het toetsen van de visie en ambitie van opdrachtgever aan de mogelijkheden welke aangeboden worden in de markt. Daarnaast diende de consultatie de markt te toetsen op de doelstellingen die opdrachtgever zich gesteld heeft, waaronder:

- De mogelijkheden tot het combineren van een audit op de BIO en AVG tot één enkele multi-normaudit;
- De beschikbare capaciteit van marktpartijen voor het uitvoeren van deze multi-norm audit voor Het Waterschapshuis, 21 waterschappen, de UvW en WBL;
- Een inhoudelijke consultatie met betrekking tot normenkaders en uitgangspunten, waarbij herhaalbaarheid van onderzoeken een aandachtspunt is;

- Een vervolg op, en relatie met, eerder uitgevoerde audits (2017: Baseline Informatieveiligheid Waterschappen, hierna: BIWA; 2018 AVG);
- Een meerjarig extern auditplan, waarbinnen self-assessments een integraal onderdeel vormen;
- Een toetsing op lerend en groeiend vermogen en voortvarende besluitvaardigheid bij opdrachtgever;
- De consistentie van audit-kwaliteit (herhaalbaarheid, vergelijkbaarheid) binnen het op te leveren meerjarenplan.

In dit verslag volgt een (geanonimiseerde) samenvatting van de gegeven antwoorden. Het betreft een samenvatting, en geen interpretatie.

2. Vragen

Organisatie van het onderzoek

2.1 Vraag 1

Is het naar uw mening mogelijk om in de uitvoering van de audit rekening te houden met de verschillende soorten en grootten van de waterschappen? Graag toelichten waarom wel of niet.

Antwoord

Marktpartijen geven aan dat het goed mogelijk is om met het uitvoeren van de audit rekening te houden met de verschillende soorten en grootten van de waterschappen. Hierbij geven zij aan dat er verschillende manieren zijn om dit op een juiste manier te doen. Allereerst moet er voorafgaand aan de audit informatie bekend zijn over de verschillende waterschappen. Verscheidende soorten informatie worden door marktpartijen genoemd waarbij sommigen ook overlappen:

- Organisatie grootte;
- Cultuurbeschrijving;
- Beschrijving organisatiestructuur;
- Complexiteit van de organisatie;
- Relevante functies/rollen in de organisaties;
- Verantwoordelijkheden en taken binnen de organisaties;
- Manier van leidinggeven;
- Het soort sturingsmodel;
- De risicobereidheid;
- De resultaatsgerichtheid;
- Het lerend en groeiend vermogen;
- De uitkomsten van eventuele nulmetingen AVG en BIWA;
- De status van BIO implementatie op dit moment.

Aan de hand van deze informatie kunnen waterschappen onderverdeeld worden. Deze onderverdeling kan volgens marktpartijen bestaan uit volwassenheidsniveaus of risicoprofielen.

Eén marktpartij draagt de mogelijkheid aan waarbij er een contextscan plaatsvindt tijdens de audit zelf op basis van een aantal van de bovenstaande informatie onderdelen. Het voordeel hiervan zou zijn dat de noodzakelijke privacy- en beveiligingsmaatregelen op een objectieve manier kunnen worden vastgesteld.

Marktpartijen gaan specifiek in op de verschillen tussen grotere waterschappen en kleinere waterschappen. Partijen zijn het erover eens dat audits bij kleinere waterschappen vermoedelijk

minder tijd kosten, omdat er bijvoorbeeld minder interviews afgenomen worden of er minder te controleren documentatie beschikbaar is. Eén partij geeft hier echter wel aan dat de benodigde functiescheiding CISO/FG lastiger te realiseren is binnen een kleine organisatie waardoor er mogelijk alternatieve beheersmaatregelen opgesteld moeten worden. Eén marktpartij geeft aan dat bij de uiteindelijke sectorscore van een audit de impact van kleinere waterschappen minder zal zijn dan het aandeel van een grotere waterschap.

Marktpartijen geven diverse tips mee om de audit zowel bij grotere als kleinere waterschappen toe te passen. Er moet op een eenduidige manier te werk worden gegaan en het moet duidelijk zijn wat de scope en object van onderzoek is per waterschap.

2.2 Vraag 2

Is het mogelijk om de waterschappen, gezien de verschillen, door middel van een onderzoek en rapportage in de leerstand te krijgen? Welke gevraagde adviesrol zou hierbij kunnen passen? Gaarne toelichten waarom juist deze adviesrol aanbevolen wordt.

Antwoord

Marktpartijen dragen verschillende plannen en werkvormen aan die kunnen bijdragen aan het in de leerstand zetten van de organisatie op het gebied van de audits. Partijen zijn het unaniem eens dat de verschillen tussen de waterschappen hierin geen probleem bij vormen. De beschreven plannen en werkvormen luiden als volgt, met daarachter tussen haakjes hoeveel marktpartijen dit punt aandragen:

- Auditrapporten worden voorzien van een verbeteradvies met daarin de behaalde verbeteringen en toekomstig te realiseren verbeteringen (6);
- Auditrapporten bevatten aandachtspunten waar medewerkers zelf verbeteringen in aan kunnen brengen. Bij een tweede meting worden de vorderingen bekeken (2);
- Audits in de vorm van self-assessment waardoor medewerkers van de verschillende waterschappen meer betrokken raken bij het onderwerp (3);
- Opzetten van acties of campagnes die de bewustwording vergroten door middel van presentaties of bijeenkomsten (2);
- Een systeem in de auditrapportage verwerken die aangeeft wat de gemiddelde prestatie is van alle waterschappen en welke waterschap(pen) op bepaalde onderdelen het best scoren en daarom als voorbeeld gezien moet worden. Dit creëert een positieve stimulans om beter te gaan presteren (2);
- De auditrapportage bevat samenvattingen en best practices(1);
- Om kennisoverdracht te bevorderen moeten de betrokken medewerkers zelf acties betrokken worden bij een passend normenkader(1);
- Het vaststellen van passende Key Performance Indicators (KPI's) per waterschap(1);
- Het weergeven van de resultaten van audits of self-assessments door middel van een dashboard(1);
- De evaluatie na de audit delen met de verschillende niveaus van betrokkenen(1);
- Een terugkomdag waarbij medewerkers die recent een audit ondergaan hebben hun ervaringen delen met de medewerkers van de andere waterschappen(1);
- 'Leerkringen' waarbij de auditor (als expert) helpt bij het formuleren van handvatten voor (gezamenlijke) uitvoering van verbeteringen(1);
- Het helpen adviseren over voortvarende besluitvaardigheid in de organisatie(1);
- Door middel van alle communicatie rondom de audits laten blijken dat het om een leerproces gaat(1);
- Een koppeling met een leersysteem van de waterschappen(1);
- Het aangaan van gezamenlijke investeringen vanuit de verschillende waterschappen(1);

- Sessies organiseren over de uitkomsten van een volwassenheidsonderzoek waarbij onderliggende oorzaken en good practices worden gedeeld tussen de waterschappen.

Een paar marktpartijen dragen ook punten aan die Opdrachtnemer moet borgen:

- Intrinsieke motivatie en flexibiliteit bij de medewerkers
- Een verantwoordelijkheidsgevoel bij de waterschappen ten opzichte van de veiligheid van hun domein

Marktpartijen benoemen verschillende adviesrollen die zij vinden passen bij deze dienstverlening. De meeste marktpartijen zien een centrale adviesrol als de juiste rol waarbij deze rol soms kan veranderen gedurende de fase van het proces. Eén marktpartij ziet de adviesrol 'expert' als een passende rol. Een expert voegt namelijk kennis en ervaring toe. Een ander marktpartij geeft aan dat zij een rol adviseert waarbij verbinden, transparantie en verbeteren. Andere rollen die genoemd worden door marktpartijen zijn ondersteunend(1) en begeleidend(1).

Zeven van de elf marktpartijen geven aan dat het zonder meer mogelijk is om naast de controlerende rol, die volgens veel partijen past bij een audit of auditor, ook de adviesrol op te pakken. Drie andere marktpartijen geven aan dat deze combinatie mogelijk is maar plaatsen wel kanttekeningen zoals:

- De adviesrol kan strijdig zijn met de auditrol wat de mogelijkheden beperkt. Geadviseerd wordt om inzet van de auditors te beperken hiervoor;
- Geadviseerd wordt om gebruik te maken van specialistisch partijen per deelgebied om potentiële belangenverstrengeling tegen te gaan;
- Geadviseerd wordt om gebruik te maken van adviseurs rondom een auditor die de adviestaken op zich nemen rondom en tijdens de audit. Deze adviseurs kunnen dan ook tijdens de audit vragen beantwoorden en praktisch advies geven. Deze adviseurs kunnen echter niet een te grote rol innemen om het eigenaarschap en het lerend vermogen niet in de weg te staan.

Eén marktpartij geeft aan dat het vaktechnisch überhaupt niet wenselijk is om de controlerende rol en de advies rol te combineren. Het belang van het een onafhankelijk oordeel zou worden ondermijnd door een grote bijkomende adviesrol. Wel kan de auditor de weg wijzen aan de waterschappen door verbetermogelijkheden aan te dragen.

2.3 Vraag 3

Is het naar uw mening mogelijk in één audit(periode) zowel de BIO als de AVG kwalitatief en volledig te auditen? Waar liggen eventuele risico's naar uw mening waar we rekening mee moeten houden bij de aanbesteding?

Antwoord

Het merendeel van de marktpartijen (10) geeft aan dat een volledige gezamenlijke BIO en AVG audit mogelijk is. Deze partijen raden het Waterschapshuis ook aan om deze audits te combineren. Deze gezamenlijke audit kan ook plaats vinden binnen één audit(periode). Eén van de marktpartijen draagt daarbij wel de mogelijkheid aan om de audit op te splitsen in twee periodes om de belasting op de verschillende organisaties en de externe partij beter te verdelen. Een bijkomend voordeel hierbij is volgens deze partij het in tweede instantie kunnen oplossen van eerder geconstateerde zaken. Deze constructie is wel kosten verhogend.

Marktpartijen dragen verschillende redenen aan waarom een gezamenlijke BIO en AVG audit mogelijk is. De redenen luiden als volgt, met daarachter tussen haakjes hoeveel marktpartijen deze reden aandragen:

- De raakvlakken tussen de BIO en de AVG zijn groot op verschillende manieren. Zo is de insteek van een beide audits een risico gebaseerde. Inhoudelijk gezien zijn de onderwerpen privacy en security sterk met elkaar verbonden. Hierbij kan de AVG gezien worden als een nadere uitwerking van het onderdeel privacy data van de security. Een bijkomend voordeel hierbij is dat het voor waterschappen duidelijk maakt op welke wijze BIO en privacy maatregelen met elkaar samenhangen. Concluderend zijn BIO en AVG complementair aan elkaar; (5)
- De combinatie leidt tot efficiëntie en effectiviteit. De organisaties en medewerkers waar de audit op ziet worden slechts een keer gevraagd naar dezelfde maatregelen die zien op zowel BIO als de AVG. Zo is geen sprake van dubbele toetsing; (3)

Daarnaast dragen de marktpartijen verschillende risico's aan waar het organisaties rekening mee moet houden. Daaraan gekoppeld zijn condities of voorwaarden waar op gelet moet worden bij een gezamenlijk BIO en AVG audit. Deze zouden ook als mitigerende maatregelen gezien kunnen worden. De risico's en maatregelen luiden als volgt, met daarachter tussen haakjes hoeveel marktpartijen deze risico's en maatregelen aandragen:

- Het ontbreken van verantwoordelijkheid en commitment bij de organisatie. Dit risico ziet op het niet aanwezig zijn van een duidelijk commitment van de bestuurlijke en ambtelijke top, gebrek aan eigenaarschap, afwezigheid van een strakke planning, onvoldoende beschikbaarheid van te interviewen functionarissen en de afwezigheid van de mogelijkheid om te escaleren binnen de organisatie. Marktpartijen adviseren om deze randvoorwaarden mee te nemen in de organisatie van de audits die, hoewel gezamenlijk effectiever, toch voor een bepaalde piekbelasting zal zorgen; (6)
- Het niet kunnen vinden van een uniform normenkader die voor alle organisaties gaan gelden. Zowel met betrekking tot BIO als AVG dragen marktpartijen aan dat de geldende normen in ontwikkeling zijn. Partijen gaan hier in de vragen 2.5 t/m 2.8 dieper op in. Marktpartijen adviseren om vooraf na te denken welke normen gehanteerd dienen te worden tijdens een audit rekening houdend met de complexiteit en verscheidenheid van de organisaties; (4)
- Het gezamenlijk uitvoeren van de BIO en AVG audit kan leiden tot de aanname dat beide audits op hetzelfde zien en het zelfde doel hebben. Dit is volgens verschillende marktpartijen nadrukkelijk niet het geval. Ten eerste zijn zowel de BIO en vooral de AVG nog in ontwikkeling waardoor in ieder geval de AVG niet als een vaste norm aangenomen kan worden. Ten tweede is er een fundamenteel verschil tussen de doelen van beide audits. De AVG ziet op verantwoord gebruik van (persoons) gegevens terwijl de BIO ziet op het veilig gebruik daarvan. Marktpartijen adviseren om, ondanks dat er meerdere gebieden zijn waar beide audits overlappen, rekening te houden met deze verschillen tijdens het opzetten en uitvoeren van de audits. Ook adviseren zij vooraf normenkaders te schetsen; (4)
- Het voorgaande punt geeft voor twee marktpartijen aanleiding om specifieke aspecten van de BIO en AVG audit te benoemen die extra aandacht verdienen tijdens een gezamenlijk audit:
 - Ten opzicht van BIO moet de PDCA cyclus en het management systeem ook meegenomen worden in de audit;
 - De AVG wetgeving en interpretatie daarvan is nog sterk in ontwikkeling en kan daarom veranderen;
 - Ten aanzien van de AVG moet er gecontroleerd worden of de mate waarin binnen verwerkingen voldaan wordt aan concrete privacy principes volstaat;
 - De AVG vraagt een ander specialisme dan de BIO. Eén marktpartij adviseert daarom om beide expertises op te nemen in een eventueel onderzoeksteam;

- De audit wordt te omvangrijk en daarom moeilijk uitvoerbaar. Hierbij wordt specifiek gedacht aan het meenemen van alle (primaire) bedrijfsprocessen, ICT-systemen en de IT-infrastructuur. De oorzaak hiervan kan liggen het feit dat er verschillende processen of IT-systemen worden gehanteerd door het Waterschapshuis, de Unie van Waterschappen en de waterschappen zelf. De oorzaak kan ook liggen in het feit dat er intern nog geen goed overzicht is welke processen of systemen en welke data daarin onderworpen is aan de BIO en de AVG. Marktpartijen adviseren om hier aan de voorkant een inschatting van te maken en desnoods de scope van de audits te beperken. IT scans kunnen bijvoorbeeld ook parallel door de waterschappen zelf opgepakt worden. Op deze manier kan de auditor meerwaarde bieden. Eén marktpartij draagt daarbij aan dat het minimaal noodzakelijk is dat de functionarissen (CISO en FG) zijn aangewezen met het juiste mandaat(3);
- De verschillen in grootte van de waterschappen en verschillen in cultuur, volwassenheid en karakteristieken van de waterschappen. Hierdoor zullen bepaalde waterschappen meer aandacht nodig hebben. Ook bestaat het risico dat kleine waterschappen onvoldoende betrokken raken bij de audits(2);
- Het uitvoeren van dubbele werkzaamheden(1);
- De BIO slecht als normenkader beschouwen en dit minder zwaar wegen als de AVG wetgeving(1);
- De verschillende die er zijn tussen deze audit en eerder uitgevoerde audits(1).

2.4 Vraag 4

Is het tijdschema en de doorlooptijd in jaren (zie 2.3) realiseerbaar voor marktpartijen?

Antwoord

Marktpartijen zijn het erover eens dat het tijdschema en de doorlooptijd haalbaar en realiseerbaar zijn voor de marktpartijen. Wel stellen marktpartijen wijzigingen in het tijdschema voor zoals:

- Eén marktpartij adviseert om af te wijken naar twee audits in plaats van vier waarbij er meer ruimte is voor het verkrijgen van een real-time inzicht in de volwassenheid van BIO en AVG. In dat geval zou de periodieke audit losgelaten moeten worden en moet daarvoor een geplande (management) aanpak terug komen;
- Een jaarlijkse audit waarbij het kalenderjaar gehanteerd wordt. Dit omdat de audit dan samenloopt met eventuele jaarlijkse control statement;
- Het opsplitsen van de audit in een pre-audit(tijdens het verslagjaar) en een reguliere audit(na afloop van het verslagjaar). Dit heeft als voordeel dat verbeterplannen beter kunnen worden meegenomen en daarnaast worden medewerkers positief beïnvloed om meer betrokken te raken bij procesverbeteringen;
- Marktpartijen hebben te maken met een piekdrukke vanwege de IT interim controles, assurance audits, ENSIA en DigiD in bepaalde periodes door het jaar heen (vaak van september t/m februari). De einddatum van 1 februari 2021 en 2022 moet daarom een harde einddatum zijn volgens één marktpartij waarbij bewijsvergaring en onderzoeken ter plaatse afgerond moet zijn. Volgens een andere marktpartij zou een looptijd tussen mei en oktober leiden tot een groter aanbod in auditors.

Daarnaast geven de marktpartijen wel een aantal aandachtspunten mee:

- Het behalen van een volwassenheidsniveau 4, waar het Waterschapshuis in drie jaar naar toe wil werken, is een ambitieuze doelstelling.
- De tijdsplanning is haalbaar mits er wordt ingegaan op een generieke opzet voor de implementatie;
- Het gaat volgens één marktpartij om een grote, tijdrovende en intensieve opdracht;
- Volgens één marktpartij geeft de planning aanleiding voor een werkwijze met een sturende adviseur op afstand. Na het inrichten van het normenkader met eventueel KPI's kunnen de medewerkers zelf beginnen met het assessment en implementeren van bijbehorende maatregelen.

Normenkader

2.5 Vraag 1

Is de AVG als kader voor de audit te gebruiken of dient een ander vergelijkbaarnormenkader te worden meegegeven bij een aanbesteding?

Antwoord

Marktpartijen geven unaniem aan de AVG geen normenkader is maar een wet en principle based geheel. Daarom is de AVG als normenkader ongeschikt. De reden hiervoor is dat de wet open staat voor interpretatie en dat deze onvoldoende is uitgewerkt in concrete maatregelen om als normenkader te fungeren. Eén marktpartij geeft aan dat de ambitie van het Waterschapshuis verder reikt dan de AVG. Marktpartijen zijn het er vervolgens over eens dat er gekozen moet worden uit een van de onderstaande normenkaders:

- Het door NOREA ontwikkelde Handreiking Privacy Control Framework;
- Het kader ISO27001/ISO27002 (ISMS) met uitbreiding van ISO27701 (PIMS).

Partijen geven aan dat deze normenkaders kunnen bijdragen aan het beoogde doel van de audit. Gezien de gezamenlijk audit AVG en BIO kunnen er naast bovenstaande normen nog losstaande normen worden toegevoegd aan het normenkader. Volgens diverse marktpartijen zijn van deze normenkaders, waterschapgerichte varianten te maken. Een nadeel van een vast toetsingskader is volgens één marktpartij dat de situationele context vaak niet wordt meegenomen.

2.6 Vraag 2

Is de BIO als normenkader toepasbaar of is een ander vergelijkbaar normenkader noodzakelijk om uit te vragen tijdens een aanbesteding?

Antwoord

Marktpartijen geven unaniem aan dat de BIO een goed en vaak gebruikt normenkader is die toegepast wordt bij audits. BIO is zo goed bruikbaar, omdat deze voor een groot deel is afgeleid uit de ISO27001. Het nadeel aan de BIO is dat het een Nederlands normenkader is terwijl ISO27001 een internationaal bekend normenkader is. BIO moet volgens de marktpartijen gezien worden als de basis voor het normenkader. Dit betekent echter niet dat het volledig is en/of dat alle aspecten die uit BIO voort komen van toepassing zijn. Eén van de marktpartijen geeft aan dat er 210 te toetsen normen volgen uit BIO en NOREA samen. Er zullen daarom keuzes gemaakt moeten worden bijvoorbeeld het hanteren van een subset aan kritieke beveiligingsnormen. De volgende extra aandachtspunten zijn van toepassing op BIO:

- Om BIO te kunnen toepassen moet helder zijn welke branche specifieke implementatierichtlijnen of handreikingen meegenomen moeten worden;
- De BIO beperkt zich tot tactische en operationele beveiligingsmaatregelen. De strategische rol van het bestuur in de organisatie en de governance komen minder aan bod. Het is daarom raadzaam om aanvullend de PDCA en governance mee te nemen bij het opstellen van een normenkader.

2.7 Vraag 3

Kent u goede voorbeelden van andere normenkaders voor zowel de BIO als de AVG? Waarom zouden deze kunnen passen bij een uitvraag?

Antwoord

De marktpartijen herhalen dat de al aangedragen opties zoals weergegeven in 2.5 en 2.6 de beste opties zijn. Daarbuiten geven zij aan dat er verschillende andere normenkaders beschikbaar zijn die raakvlakken hebben met de uitvraag. Marktpartijen dragen de volgende normenkaders aan voor zowel BIO als de AVG:

- Cloudmatrix wanneer er op het gebied van SaaS/Cloud een relatie gelegd moet worden tussen verschillende normkaders;
- Om de werking van bepaalde maatregelen aan te tonen is een normenkader uit de SOC2/ISAE-familie goed bruikbaar;

- Op security gebied de Amerikaanse normen NIST 800-53, NIST 800-171 en DFAR;
- De ABDO dat geldt als normenkader voor de Nederlandse defensie industrie;
- NIST cybersecurity framework (NIST CDF) met betrekking tot de kritieke infrastructuur. En specifiek daaronder de NIST 800 SP 53 Security and Privacy Controls for Federal Information Systems and Organizations;
- ISO27005 voor het naleven van richtlijnen met betrekking tot informatieveiligheidsrisicomanagement;
- Privacy Central Framework (VNG) waar de AVG is vertaald voor gemeentes naar een kwaliteitscyclus voor gegevensbescherming en privacy;
- ISO33020 welke ziet op hoe de werking van een volwassenheidsproces meetbaar te maken is.

Hiernaast dragen marktpartijen ook nog een aantal wetten of rapporten aan die meegenomen moeten/kunnen worden bij het opstellen van normenkaders:

- De Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) ziet op vitale sectorwetgeving die ook van toepassing lijkt op Waterschappen en Hoogheemraadschappen;
- Regels met betrekking tot gebruik van Amerikaanse technologie zoals Microsoft Office, Windows 10, Google en Android;
- Regels afkomstig van de European Data Protection Board (EDPB);
- NOREA studierapport "Algemene beheersing van IT-diensten.

2.8 Vraag 4

Een recent voorbeeld van een kader is de ISO27701 voor de privacy/AVG. Hoe staat u hier tegenover en wat is uw advies in deze?

Antwoord

De marktpartijen staan unaniem positief tegenover het gebruik van ISO27701 voor privacy/AVG. Zij geven nogmaals aan dat dit normenkader een uitbreiding vormt op ISO27001 waar de BIO uit afgeleid is. Dit nieuwe normenkader is specifiek gericht op de privacy component van informatiebeveiliging en implementeert op deze wijze de AVG in een normenkader. Op deze manier geeft dit normenkader de mogelijkheid om de AVG beter te integreren in het auditproces. Een aantal marktpartijen geven wel overwegingen mee bij het gebruik van dit normenkader:

- Het normenkader moet geen doel op zich worden maar is een basis waaruit verder gebouwd kan worden. Als top wordt gegeven om het NOREA-kader als cross-referentie te gebruiken;
- Het normenkader gaat onvoldoende in op het managementsysteem;
- Het normenkader dekt de AVG niet volledig af omdat de onderwerpen grondslag/doelbinding, minimalisatie en transparantie niet voldoende zijn uitgewerkt;
- Dit normenkader is vooralsnog Engelstalig. Eén marktpartij adviseert om het normenkader pas te gebruiken wanneer daar een Nederlandstalige vertaling gereed is.

Kwaliteitsborging van het onderzoek

2.9 Vraag 1

Waterschappen vormen een specifieke overheidssector en dat vraagt specifieke kennis van de onderzoekers. Wat is naar uw mening nodig om het onderzoek kwalitatief goed uit te kunnen voeren? Ofwel, welke kwaliteitseisen zouden wij moeten stellen aan de onderzoekers?

Antwoord

Marktpartijen dragen verschillende aspecten aan waar onderzoekers aan zouden moeten voldoen. Deze aspecten luiden als volgt, met daarachter tussen haakjes hoeveel marktpartijen aspecten aandragen:

- Bewezen ervaring in het begeleiden van publieke organisaties in het verbeteren van het informatiebeveiliging- en privacy domein. Hieronder valt specifiek advisering en kennis van

verschillende normenkaders. Om voorbeeld om dit te testen is om CISM, CISSP, CIPPE of CIPM certificaten uit te vragen; (7)

- Gekwalificeerd in het uitvoeren van objectief en herhaalbaar onderzoek. Hieronder valt het uitvoeren van audits door gekwalificeerde auditors (op bijv. RE en CISA); (6)
- Kennis van de waterschapsector en inzicht in de verhoudingen tussen HWH, UvW en de waterschappen. Dit kan meetbaar gemaakt worden door een percentage van de waterschappen uit te vragen waarvoor inschrijvers werkzaamheden hebben verricht; (4)
- Kennis van de vitale infrastructuren en werking van organisaties in een politiek sensitieve omgeving; (3)
- Brede kennis en ervaring op het gebied van maatregelen van de BIO en de toepasbaarheid en implementatie binnen overheidsorganisaties; (3)
- Ervaring en affiniteit met de AVG; (2)
- Het kunnen hanteren van auditstandaarden zoals IFAC of NOREA voor het uitvoeren van zorgvuldige audits(1);
- Het opereren van auditors in vaste teams(1);
- Ruime ervaring in het implementeren van informatiebetrouwbaarheid en privacybeschermende maatregelen(1);
- Ervaring met het Capability Maturity Model (CMM) en kunnen integreren binnen bedrijfsprocessen(1);
- Communicatief en analytisch vaardig(1);
- Sociaal en empathisch met betrekking tot de begeleidende en adviserende rol gedurende de audits(1);
- Kennis met betrekking tot de hedendaagse techniek(1);
- Kennis van ICS/SCADA omgevingen, de risico's en de beveiliging daarvan(1);
- In staat om het veranderproces bij organisaties te ondersteunen(1).

2.10 Vraag 2

Hoe zou u zelf de kwaliteit van het onderzoek eventueel borgen (meerdere teams, eenheid in beoordeling etc.)?

Antwoord

Marktpartijen hebben op een verschillende manier antwoord gegeven op deze vraag. Een aantal partijen geven op dit onderdeel aan wat voor soort team zij aandragen om de kwaliteit te waarborgen en hoe deze teams te werk gaan. Een aantal voorbeelden hiervan zijn:

- Een klein of compact gespecialiseerd team met een standaard auditaanpak en een standaard werkprogramma. In deze teams zijn de functies helder verdeeld is precies duidelijk wie voor welk onderdeel aan zet is en de kennis in huis heeft;
- Een team waarin zowel proceskennis als inhoudelijk informatiebeveiliging/privacy expertise aanwezig is;
- Verschillende teams met een gelaagde structuur waardoor altijd het juiste team naar voren geschoven kan worden passend bij de complexiteit en de vereiste deskundigheid;
- Eén team werkt met meerdere IT-auditors om de kwaliteit en de kennis op een hoog niveau te brengen en te houden. Dit wordt versterkt door specifieke trainingen, tussentijdse themasessies, wekelijks overleg en gestandaardiseerde dossiervorming;
- Een multidisciplinair team waar zowel consultancy-ervaring, audit-ervaring en ondersteuning in aanwezig is.

Overige aandachtspunten die marktpartijen aandragen bij de beschrijving van de kwaliteitsborging en de in te zetten teams:

- Interne controle van auditors wordt door verschillende marktpartijen aangedragen. Hier zijn verschillende bewoordingen voor zoals het '4-ogen principe' en 'Quality Control';
- Het betrekken van materiedeskundigen van de waterschappen bij het uitwerken van de onderzoeksanpak en het toetsingskader;
- Afstemmen van rapportageformats met de waterschappen;

- Aanstellen van een centrale onderzoeksleider die aanpak aanstuurt en bewaakt, de consistentie tussen bevindingen bewaakt en die de eindresultaten overziet;
- Een beperkt aantal mensen inschakelen voor onderzoeken om het lerend vermogen aan de kant van de auditors zo groot mogelijk te maken;
- Uitwisselen van ervaringen en bevindingen gedurende de onderzoeken;
- Teams moeten nauw in contact staan met de functionaris gegevensbescherming (FG);
- Een consultant die altijd beschikbaar is wanneer de waterschappen hulp nodig hebben bij de self-assessments;
- Kwaliteitsborging wordt opgevangen door periodieke intervisie audit teams;
- Een gedegen dossierreview;
- Collegiale question & answer sessies.

2.11 Vraag 3

Vraagt het meerjarig karakter van de opdracht (2020-2023) specifieke aandachtspunten over de kwaliteit bij de uitvraag? Dit in relatie tot de herhaalbaarheid van de onderzoeken.

Antwoord

Marktpartijen zien de volgende specifieke aandachtspunten met betrekking tot de kwaliteitsborging bij een opdracht met een meerjarig karakter (2020-2023):

- Om in de 2^e auditronde de “werking” van de beveiligingsmaatregelen en privacy-bevorderende maatregelen te laten beoordelen moet er in de eerste ronde precies aangegeven worden welk bewijsmateriaal wordt verwacht om de “werking” te kunnen vast stellen;
- Dit vereist een duidelijk roadmap;
- Een langere looptijd ziet op het feit dat de herhaalbaarheid van de maatregelen na verloop van tijd niet afhankelijk is van een auditor maar ook vaststelling via zelfevaluaties;
- Het doel dat de opdrachtgever met de audits heeft, moet ten allen tijde met opdrachtnemer worden gedeeld, ook wanneer deze wijzigt;
- Normenkaders en maatregelen moeten gedurende de looptijd van de opdracht eenduidig worden uitgelegd om aan het eind resultaten te kunnen halen;
- Het meerjarige karakter in combinatie met de positie van de waterschappen brengt met zich mee dat de opdracht ook gezien moet worden als een groeimodel;
- Er moet ruimte zijn om in goed overleg aanpassingen te verrichten aan het onderzoeksvoorstel om deze in een later stadium passend en actueel te houden;
- Het is belangrijk dat de verantwoordelijkheden die gekoppeld zijn aan bepaalde functies moeiteloos vervangen kunnen worden;
- De eisen aan de volwassenheidsniveaus moeten gelijk blijven om de kwaliteit te waarborgen;
- Het meerjarige karakter vraagt om kwalitatief goede en volledige dossiervorming tijdens en na elke audit.

Volwassenheidsniveaus

2.12 Vraag 1

Kunnen de waterschappen naar uw mening getoetst worden op door ons geformuleerde volwassenheidsniveaus? Graag toelichten waarom wel/niet.

Antwoord

Marktpartijen reageren verschillend op deze vraag. Een deel van de marktpartijen geeft aan de waterschappen wel op deze manier getoetst kunnen worden⁽⁹⁾. Zij dragen daarbij de volgende toelichting of kanttekeningen aan:

- Het is een landelijk uitvoerbaar systeem die met een paar kleine aanpassingen op kwalitatief gebied geschikt is voor de waterschappen;
- Het is mogelijk na een herijking van de CMM methode;
- De CMM methode is een meetlat die volgens één marktpartij op alle genoemde waterschap organisaties van toepassing is;
- Eén partij geeft aan dat methode mogelijk is maar draagt veel zaken aan die eerst verandert moeten worden zoals de identificatie van de normen, de onderlinge samenhang en weging van de onderdelen 'monitoring', 'onderbouwing', 'mensen' en 'inrichting' moet verder worden uitgewerkt. Ook moet er gedacht worden aan de verscheidenheid in soort en omvang van de waterschappen;
- Volgens één marktpartij biedt de methode zeker handvaten om een toetsing op uit te voeren of in ieder geval om conclusies op te trekken. Deze marktpartij ziet echter wel graag dat de toetsing verder gaat dan de volwassenheidsniveaus. Inhoudelijk ziet deze marktpartij ook graag een toetsing op de informatiebeveiliging en privacy zelf;
- Eén marktpartij draagt aanvullend aan dat een cross referentie op basis van NOREA en BIO de verschillende waterschappen kunnen plotten om het voorgestelde model. Het is hierbij van belang dat er rekening gehouden wordt met de verschillen tussen de waterschappen;
- Eén marktpartij plaatst een belangrijke kanttekening bij het model van volwassenheidsniveaus. Omdat het gaat om het lerend vermogen van waterschappen heeft het weinig zin om een waterschap dat zich op een laag niveau bevindt te onderwerpen aan aanbevelingen die zien op een volwassenheidsniveau 4. De marktpartij adviseert individuele waterschappen perspectief te bieden door steeds kleine stappen vooruit te maken. Dit verhoogd de acceptatie van het leerproces bij de waterschappen.

Een aantal marktpartijen zien de CMM methode niet als een toepasbare methode voor de waterschappen en geven daar de volgende redenen voor(2):

- De informatiebetrouwbaarheid wordt in zijn geheel niet door vertaald naar normering op de verschillende onderdelen bij de voorgestelde methode. Hierdoor is het niet bruikbaar. Om deze methode tot een succes te maken moet en vooraf een duidelijk definitie van de verschillende niveaus gemaakt worden, waardoor een objectief toetsingskader ontstaat waartegen de audit kan worden uitgevoerd. Een systeem/methode waar dit in ieder geval al wel mogelijk is, is het COBIT normenkader. Deze is om te zetten naar de BIO.
- De diverse onderdelen zijn onvoldoende SMART geformuleerd en er ontbreken uniforme toetsingscriteria. Geadviseerd wordt om te kijken naar een CMMI-model of INK-model. Ook het Privacy Volwassenheidsmodel van het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) is een optie.

2.13 Vraag 2

Gelet op de verschillende soorten en grootten van de waterschappen is 1 niveau wel toepasbaar voor de onderlinge vergelijking?

Antwoord

De marktpartijen geven verschillend antwoord op deze vraag. Een deel van de marktpartijen geeft aan dat dit mogelijk is en aantal van hen dragen daarbij ook aanbevelingen aan(7). Waarom is het mogelijk:

- Het minimale volwassenheidsniveau van de waterschapssector, die bij de Nederlandse vitale infrastructuur behoren, moet volgens één marktpartij hoger dan 3 zijn. De waterschappen zullen daarom vroeg of laat deze route in moeten slaan. Rekening houdend met de verschillende aspecten van de organisaties is dit volgens deze marktpartij mogelijk.
- Een aantal partijen geven aan dat één niveau zowel voor de roadmap en te behalen KPI's als voor de toetsing zelf wenselijk is. Echter kan over het te behalen niveau getwist

worden. Twee marktpartijen geven daarbij aan dat niveau 3 wellicht meer voor de hand ligt dan niveau 4.

De aanbevelingen die marktpartijen aandragen:

- Diverse factoren zorgen mogelijk voor een disbalans in de groei naar eenzelfde volwassenheidsniveau zijn:
 - De verschillen in grootte van de waterschappen;
 - De verschillen in cultuur en karakteristieken;
 - Verschillen in mate van opvolging van eerder uitgevoerde audits voor de BIWA en AVG;
 - Gebrek aan kennis en kunde binnen de waterschappen;
 - Gebrek aan beschikbare tijd en planning binnen de waterschappen;
 - Onjuiste en onvolledige opvolging procesimplementatie;
 - Gebrek aan eigenaarschap.
- Er moet op een verstandige manier omgegaan worden met de audits waarbij individuele best practices van waterschappen die niet overeenkomen met een gangbare maatregel maar wel het risico afdekt ook meegenomen moeten worden in de toetsing. Een bepaalde proportionaliteit moet op dit punt gelden.

Een deel van de marktpartijen blijft in het midden(2) of keurt 1 niveau voor alle waterschappen af(2). Partijen geven ook aan waarom dit niet mogelijk zou zijn is:

- Er dient eerste een benchmarking plaats te vinden onder de waterschappen alvorens er een inschatting gemaakt kan worden of 1 niveau haalbaar is. Daarbij is het goed om mee te nemen volgens de marktpartij dat het niet wenselijk is dat er niveau worden overgeslagen en dat een volwassenheidsniveau passend dient te zijn voor de aard en omvang van de organisatie. Daarom is het niet verstandig om met 1 niveau te werken.
- Een tussenoplossing wordt vervolgens nog aangedragen door één marktpartij. Te denken valt het opdelen van alle waterschappen in 2 of drie categorieën. Een derde optie is het handteren van een groeimodel. Dit wordt verder niet onderbouwd.

2.14 Vraag 3

Kunt u de waterschappen helpen om het theoretische volwassenheidsstandaard CMM binnen de auditrapporten naar de praktijk van waterschappen te vertalen om benodigde herkenbaarheid bij een waterschap te verkrijgen?

Antwoord

De marktpartijen zijn het unaniem eens dat de theoretische volwassenheidsstandaard CMM goed te vertalen is naar de praktijk van de waterschappen om op die manier herkenbaarheid bij een waterschap te verkrijgen. Veel partijen geven aan hier verschillende methodes of tools voor in huis hebben maar dat dit ook sterk afhangt van de vorm waarin het Waterschapshuis dit wil laten plaatsvinden. Een aantal partijen dragen specifiek voorbeelden aan hoe de vertaling gemaakt kan worden:

- Het organiseren van leerkringen/workshops kan hier een bijdrage aan leveren. Om medewerkers tijdens deze bijeenkomsten te betrekken bij conclusievorming laten helpen bij het bedenken van vervolgstappen ontstaat er begrip en eigenaarschap bij de eigen organisatie;
- De mens als component goed meenemen in de weergave van de volwassenheidsstandaard;
- De groei naar hogere volwassenheidsniveaus kan weergegeven worden dankzij data-analyses en data views;
- Een opsomming van de belangrijkste conclusies en aandachtspunten samengevat in een management letter;

- Duidelijk maken aan iedere betrokken werknemer wat de huidige positie is maar ook wat nog gedaan moet worden om een volgend niveau te bereiken;
- Het projectteren van een overzicht van de voortgang per waterschap. Vergelijkend materiaal kan veel duidelijk maken;
- Het stimuleren van medewerkers.

Auditcyclus

2.15 Vraag 1

Onze auditcyclus is beschreven in de gewenste situatie. Is dit in aanvulling op de vraag bij de kwaliteit, realiseerbaar voor marktpartijen?

Antwoord

De marktpartijen zijn het unaniem eens dat de auditcyclus zoals beschreven in de gewenste situatie realiseerbaar is. Er is slecht één marktpartij die aangeeft dat een bepaald onderdeel niet tijdig afgerond kan worden, namelijk de rapportage na de cyclus op de gewenste termijn. Marktpartijen zien wel in dat alles soepel moet verlopen om de planning realiseren. Zij merken daarbij het volgende op:

- De grootste uitdaging zit volgens één leverancier in het logistiek plannen van cyclus en de vertaling “naar werking” in de tweede cyclus.
- Eén marktpartij geeft aan dat het gewenste niveau van de volwassenheid niet altijd hetgeen is wat aangetroffen wordt. Het verschil daartussen is een GAP en deze zal overbrugd moeten worden wat op zichzelf weer tijd kost.
- Eén marktpartij geeft aan dat hij nog geen goede inschatting kan maken van de haalbaarheid van de auditcyclus omdat dit volgens hem afhankelijk is van de nulmetingen van de waterschappen. Het is te kort door de bocht om gegevens over te nemen van een voorgaande auditronde;
- De planning wordt gezien als haalbaar maar zeer ambitieus;
- Het werken in een multidisciplinair team, het starten met een gedegen plan van aanpak en het vastleggen van governance zijn noodzakelijk om kwalitatief goed te werk te gaan. Dit ook voor de haalbaarheid van de cyclus van groot belang;
- Het succesvol uitvoeren van self-assessments draagt bij aan de haalbaarheid van de cyclus;
- Om de cyclus te realiseren heeft het Waterschapshuis een opdrachtnemer nodig die op operationeel, tactisch en strategisch niveau mee kan denken met de waterschappen en daarnaast voldoende tijd heeft om een langdurige audit uit te voeren.

2.16 Vraag 2

Hoe denkt u over de gewenste toets op de werking die gepland staat in 2022, voor onze situatie?

Antwoord

De marktpartijen onderscheiden verschillende zaken als het gaat om de werkingstoets.

Een werkingstoets ziet volgens de marktpartijen op een toets die controleert of de organisaties op dat moment in staat zijn om processen te introduceren, beheersen en meetbaar te maken waarbij de informatiebeveiliging gegarandeerd kan worden. Partijen zijn het er over eens dat een toetsing zonder een werkingstoets aan het eind veel van zijn kracht verliest. Op het moment dat de werking getoetst wordt kan opdrachtgever controleren of procedures ook zijn opgezet en bestaan/geïmplementeerd zijn. Marktpartijen zijn het er ook over eens dat een werkingstoets voor volwassenheidsniveau 4 een grondige betreft. Niet alle marktpartijen gaan daar verder op in, maar

één partij geeft aan dat het een heel jaar 'in control' betreft en een andere partij geeft als voorbeeld dat er steekproeven gehouden zullen worden op dataregisters. De centrale vraag die het Waterschapshuis moet beantwoorden is wat het doel is van de werkingstoets. Wanneer het doel is om processen kwalitatief te optimaliseren en de werkingstoets daarmee als een leertoets beschouwd wordt, dan is dat prima mogelijk. Echter, wanneer opdrachtgever foutloos de werkingstoets niveau 4 wil doorstaan om zo een certificaat te behalen zal er ook op eenzelfde manier gepresteerd moeten worden.

Naast deze hoofdvisie zijn er nog een aantal andere antwoorden op deze vraag:

- De meeste marktpartijen zien de werkingstoets beginnen tussen de 1^e en 2^e audit.
- De werkingstoets kan voorafgegaan worden door een sessie waarin duidelijk wordt uitgelegd wat de bedoeling is en waar op getoetst zal worden;
- De ervaring bestaat bij één marktpartij dat onvolwassen organisaties vaak negatief scoren op formele aspecten. Dit wil zeggen dat er inhoudelijk was een maatregel is genomen maar dat deze maatregel niet conform de juiste norm is toegepast. Het is daarom te adviseren om bij het scheppen van een normenkader de inhoud voorop te zetten;
- Er zal een piekbelasting zijn van zowel de auditors als de organisaties tijdens de werkingstoets;
- Eén marktpartij adviseert het Waterschapshuis om vooraf goed helder te hebben wat de scope van de audit moet zijn en hoe deze scope zich verhoudt tot het gewenste resultaat.

2.17 Vraag 3

Kunt u een groeipad en adviezen meegeven in de aanbevelingen van de toetst op opzet en bestaan?

Antwoord

Ja dit is mogelijk voor marktpartijen. Zij gaan daar verder op met randvoorwaarden en handvaten:

- De bevindingen in een auditrapport kunnen richtinggevend geformuleerd zijn zonder dat dit de scheidslijn tussen een audit en een advies overschrijdt.
- Als input voor de adviezen geven marktpartijen alvast het volgende mee:
 - Beperk de processen die elk waterschap uitvoert tot de zogenaamde "common body";
 - Beperk de scope tot die controls die essentieel zijn voor de leercurve en het meest risico vormen voor de vitale infrastructuur;
 - Beslis aan de voorkant of u technisch onderzoeken, netwerkscans en penetratietesten wel of niet tot de scope rekent;
 - Start met een nulmeting en kijk of er een GAP in beeld is of juist niet;
- Aan het begin van het groeipad is het volgens één marktpartij zaak om een leerkring op te starten en aansluiten bij eerdere audits en/of een eerder uitgevoerde nulmeting;
- Eén marktpartij geeft als tip om de drie onderdelen opzet, bestaan en werking juist niet te splitsen maar deze integraal op te pakken;
- Meerdere marktpartijen geven aan dat zij graag met het Waterschapshuis in gesprek gaan over een groeipad en hoe deze eruit moet komen te zien;
- Eén marktpartij stelt voor om wanneer een nulmeting een lage mate van volwassenheid laat zien, het groeipad naar 2022 bijgesteld dient te worden naar enkel opzet en bestaan. Wanneer de nulmeting een hoge volwassenheid laat zien dan kan er in 2022 gestart worden met een toetsing op de werking;
- Eén marktpartij adviseert om te denken in kleine stappen. Dit maakt de vervolgacties overzichtelijk, behapbaar en realiseerbaar;
- Eén marktpartij stelt voor om het onderdeel werking met een jaar op te schuiven zodat er voldoende tijd is en er toch een werkingstoets kan plaatsvinden;

- Eén marktpartij geeft wel aan dat in het geval van een gewenste 'derde verklaring' aan de hand een audit, het voor de auditor lastig is om ook nog adviezen te verweven in zijn toetsingsrapport. De onafhankelijkheid komt dan in het geding.

Kosten

2.18 Vraag 1

Met welke te verwachten kosten dienen wij rekening te houden voor de auditcyclus op opzet en bestaan?

Antwoord

Gezien de gevoeligheid en ontvangen bedrijfseconomische gegevens, zal aanbestedende dienst hier geen nadere informatie over verstrekken.

2.19 Vraag 2

En voor de auditcyclus op opzet, bestaan en werking? Met welke aanvullende kosten, t.o.v. de vraag hiervoor, moet rekening worden gehouden als opdrachtgever tevens de 'werking' wil laten toetsen?

Antwoord

Gezien de gevoeligheid en ontvangen bedrijfseconomische gegevens, zal aanbestedende dienst hier geen nadere informatie over verstrekken.