Volgnr.	Vraag	Antwoord
1	Zijn alle maatregelen vanuit de ISO/IEC 27001 en BIO van toepassing verklaard?	Nee. Zie ook vraag en antwoord 2.
2	Kunt u de Verklaring van toepasselijkheid voor zowel de ISO/IEC 27001 als de BIO beschikbaar stellen?	Bij de eerste inventarisatie lijken 8.04, 8.25, 8.28 en 8.30 niet van toepassing te zijn. Deze staan dan ook in de voorlopige VVT.
3	Dienen vereisten (voor zover nu bekend) vanuit de NIS2 meegenomen te worden tijdens de audit?	Nee.
4	De scope van de audit betreffen de door VNG geïdentificeerde kritieke processen. Heeft de gemeente de volledige scope voor haar eigen situatie in kaart (processen, applicaties en onderliggende infrastructuur)? Kan dit bij een eventuele aanbesteding/opdracht opgenomen worden in de aanbestedingsdocumenten?	Aan het in kaart brengen van de processen, de informatie die hierin wordt verwerkt en de applicaties die daarbij gebruik worden, wordt gewerkt.
5	De BIO2-kritieke processen worden in de praktijk ondersteund door een grote hoeveelheid applicaties. Een aantal ISO 27001-maatregelen dienen per applicatie te worden beoordeeld, vooral bij het toetsen van de werking. Hoe denkt de gemeente deze scope praktisch af te bakenen, zodat de auditinspanning beheersbaar blijft? Is er bijvoorbeeld een overzicht beschikbaar van applicaties per proces of worden er selectiecriteria gehanteerd?	Per proces zal dit het geval zijn, maar naast vakapplicaties zullen generiekere applicaties bij meerdere processen voorkomen waardoor het aantal unieke applicaties lager zal uitvallen. Zie voor de beschikbaarheid van een overzicht het antwoord op vraag 4.
6	Zijn alle ISO onderdelen en overheidspecifieke maatregelen (BIO) van toepassing. Heeft de gemeente dit gedefinieerd in een Verklaring van Toepasselijkheid (Statement of Applicability)?	Nee, bij de eerste inventarisatie lijken 8.04, 8.25, 8.28 en 8.30 niet van toepassing te zijn. Deze staan dan ook in de voorlopige VVT.
7	In het auditplan is een cyclische dekking van alle onderdelen opgenomen, zodat over 3 jaar tijd alle onderdelen geraakt worden. Het jaarlijks beoordelen van het ISMS moet borgen dat belangrijke risico's niet te laat in scope komen. Overweegt de gemeente om bijvoorbeeld hoge risico-onderdelen ieder jaar inhoudelijk in de interne audit mee te nemen i.p.v. één keer in de drie jaar? In hoeverre is dit auditplan al definitief?	We volgen voor de eerste drie jaar het voorbeeld van de informatiebeveiligingsdienst.
8	Heeft de gemeente rekening gehouden met de overlap met ENSIA en hierin reeds beslissingen genomen ten aanzien van mogelijke overlap van auditwerkzaamheden?	De auditresultaten worden gebruikt om betreffende ENSIA-vragen over de BIO2 te beantwoorden.
9	In het marktconsultatiedocument wordt gesproken over het uitvoeren van interne audits op het ISMS van de gemeente. Kunt u bevestigen of er momenteel een operationeel ISMS aanwezig is binnen de gemeente Bergen op Zoom? Zo ja, kunt u aangeven in welke mate dit ISMS al is ingericht conform ISO 27001 en of er al eerdere interne of externe audits hebben plaatsgevonden?	Er is een ISMS aanwezig. Dit is echter nog niet compleet en daarom wordt er momenteel gebouwd aan het opzetten/uitbreiden van het ISMS. We volgen hiervoor zoveel als mogelijk de handreikingen en voorbeelden van de informatiebeveiligingsdienst die gebaseerd zijn op de ISO27001 en BIO2.
10	Om een realistische inschatting van de benodigde inspanning te kunnen maken, is het van belang te weten hoe de ISMS-audit organisatorisch wordt ondersteund. Kunt u aangeven of er een operationeel ISMS aanwezig is met centrale en actuele documentatie? Daarnaast vernemen wij graag via welke contactstructuur de audit zal verlopen (bijv. via één centrale contactpersoon of per afdeling), en welke afdelingen of functionarissen doorgaans betrokken zijn bij het aanleveren van auditinformatie.	Zie beantwoording vraag 9. De audit zal verlopen via één centrale contactpersoon. Voor het aanleveren van de auditinformatie zijn met name de afdelingen Informatisering & Automatisering, Facilitair en HRM betrokken.
11	Kunt u toelichten hoe de ICT- en informatiebeveiligingsfunctie binnen de gemeente Bergen op Zoom is georganiseerd? Worden deze functies intern uitgevoerd, zijn ze uitbesteed aan externe dienstverleners of vallen ze onder een samenwerkingsverband? Indien sprake is van externe partijen, vernemen wij graag of de interne audit ook deze externe onderdelen dient te omvatten. Of wordt in dat geval gesteund op (assurance)verklaringen van deze externe partijen?	De ICT-functies zijn belegd in de afdeling Informatisering & Automatisering en is onderdeel van de directie bedrijfsvoering. Binnen deze afdeling zijn twee (technische) ISO's werkzaam. De CISO is onderdeel van de staf-afdeling Control & Audits. We maken (uiteraard) gebruik van externe partijen, maar niet specifiek voor informatiebeveiligingsfuncties. Voor zover we gebruik maken van externe partijen wordt voornamelijk gesteund op ISO27001-certificaten van die partijen.
12	Er staat in jaar 3 voorbereiding op de externe certificeringsaudit (indien van toepassing). Wat is de ambitie van Bergen op Zoom? Hoe waarschijnijk is het dat er eind jaar 3 ook een certificering plaats gaat vinden?	Die ambitie is nog niet bepaald. Deze zal mede afhangen van de extra kosten van certificeren en verantwoordingslast voor de organisatie bovenop de uit te voeren interne audit.
13	Ziet de gemeente certificering als een logisch vervolg op de interne auditcyclus of als een los traject?	Certificering kan een logische stap zijn als vervolg van de interne audit cyclus.
14	Na elke audit wordt een actieplan opgesteld: doet de gemeente dat zelf op basis van bevindingen van de auditor of wordt daar ondersteuning van de dienstverlener gevraagd ?	Dit doen wij zelf op basis van de auditresultaten.
15	Hoe is de afdeling Control & Audits gepositioneerd en is er een onafhankelijk kanaal naar bestuur geborgd?	De afdeling Control & Audits is als stafadeling gepositioneerd onder de gemeentesecretaris.
16	Is er een overzicht van de status van huidige BIO(2) maatregelen dan wel ISMS maatregelen?	Deels, vanuit de self assessment BIO uit de ENSIA.
17	U geeft aan dat u de nieuwe hoofdstukken van annex A over drie jaar wilt spreiden: wat wordt hiermee bedoeld?	Zie BIO2 Handreiking ISMS van de informatiebeveiligingsdienst, bijlage 3: Meerjaren interne audit programma
18	Zijn er recent interne of externe audits uitgevoerd op informatiebeveiliging?	Nee, alleen de jaarlijkse self assessment op basis van ENSIA
19	De scope zijn de kritieke processen zoals gedefinieerd door IBP. Blijft deze scope voor de drie jaar gelijk?	De scope kan wijzigen, voor nu gaan we uit van de kritieke processen zoals gedefinieerd door de informatiebeveiligingsdienst.
20	Voor de scope: de door het IBP bepaalde ' overige processen' bevat de onderdelen bedrijsvoering facilitair en ISMS. In hoeverre zijn deze uit scope?	Alleen de processen op het Excel tabblad "kritieke processen" vallen binnen de scope.
21	Zijn er externe partijen die binnen de scope vallen?	Nee. Een belangrijk deel van de ICT is uitbesteed aan een externe partij. Deze heeft een ISO27001 certificering waarop wij leunen.
22	Hoe wordt er mee omgegaan als de spreiding van control testing over de jaren wordt herzien of verzwaard op basis van resultaten van risicoanalyses en interne audit resultaten? En kan er in dat geval afgeweken worden van een vooraf afgestemde hoeveeheid uren inzet van de auditor?	We willen niet afwijken van het auditplan. De ervaring met de eerste drie jaren zal leren hoe we hier in de toekomst mee willen omgaan.
23	Wordt op dit moment al de effectiveit van maatregelen gemeten? Zo ja, op welke wijze en is dit beschikbaar voor de auditor?	Dit gebeurt nu nog beperkt, daar waar dit door externe vereisten verplicht is. Denk daarbij aan DigiD, Suwinet en Wpg.
24	Scope van ISMS zijn de kritieke processen zoals weergegeven: is de verwachting dat deze scope gelijk blijft voor drie jaren, kan dat worden gegarandeerd?	De scope kan wijzigen, voor nu gaan we uit van de kritieke processen zoals gedefinieerd door de informatiebeveiligingsdienst.

25	De jaarlijkse rapportage met bevindingen en aanbevelingen wordt niet vereist in een formele assurance standaard, maar mag in de vorm van een intern beoogde adviesrapportage? Kunt u dat bevestigen of anders aangeven volgens welke vaktechnische standaard u het rapport wenst?	Dit kunnen we bevestigen.
26	Hoe zal het rapport worden verspreid? Kunt u bevestigen dat de auditrapportage alleen intern is bedoeld en niet verstrekt zal worden aan externe partijen?	Digitaal of op papier. Nee, we kunnen niet bevestigen dat de auditrapportage alleen intern bedoeld is.
27	Zijn er verdere eisen aan de rapportagevorm van de bevindingen zoals heatmaps of dashboards?	Nee.
28	Verwacht u van de auditor ook input voor college van B&W of gemeenteraad?	Nee.
29	Jaarlijkse management review : wat wordt daar verwacht van de interne auditor	De auditresultaten moeten gebruikt kunnen worden als input voor de managementreview. Verder wordt geen inzet verwacht van de auditor.
30	Wie monitort de realisatie van de actiepunten en verwacht u hier tussentijds nog ondersteuning van de auditor? Zo ja, in welke vorm?	Dat doet wij zelf en wij verwachten daarbij geen ondersteuning van de auditor.
31	Wat is de rol van CISO en Control & Audits in het auditproces?	De CISO, onderdeel van Control & Audit, organiseert en faciliteert de audit.
32	Zijn er specifieke eisen aan de onafhankelijkheid van de interne auditor?	Ja, zie de eisen die voortvloeien uit de Cyberbeveiligingswet.
33	Gaat het over de jaren 25-26-27?	Het betreft de jaren 2026, 2027 en 2028.
34	Welke tooling gebruikt de gemeente voor ISMS-documentatie en risicobeheer?	Mavim
35	Is er overlap tussen de scope van het ISMS en andere managementsystemen?	Het ISMS maakt gebruik van een GRC-tool waarvan ook proces- en risicomanagement onderdeel van zijn.
36	Hoe wordt de auditor tijdig geïnformeerd over wijzigingen in scope of organisatie?	Via e-mail of telefonisch.
37	Welke kwaliteitsaspecten zijn voor de gemeente het belangrijkst bij de uitvoering van de audit?	Belangrijkste kwaliteitsaspect is de toetsing op opzet, bestaan en werking van maatregelen. Daarbij zijn een audittrail en de van toepassing zijnde normenkaders van belang.
38	Hoe wordt geborgd dat de auditor voldoende toegang krijgt tot relevante informatie en systemen?	Door zorgvuldige planning en scopebepaling.
39	Is er ruimte voor een proactieve adviserende rol van de auditor buiten de auditrapportage om?	Nee, hooguit in de vorm van richtinggevend advies hoe te komen tot een positieve auditbeoordeling.
40	Hoe wordt omgegaan met weerstand of beperkte medewerking vanuit afdelingen?	Het auditplan en daarmee de audit zal alleen uitgevoerd worden met goedkeuruing van het seniormanagement om draagvlak te borgen.