

Marktconsultatie

“Interne ISO 27001 audit”



1. Inleiding

1.1. Algemeen

De gemeente Bergen op Zoom heeft de behoefte om de markt met betrekking tot het uitvoeren van interne audits op ISO 27001 te verkennen om tot inzichten, suggesties en ideeën te komen voor een actuele en marktconforme aanbesteding.

Teneinde onderbouwde keuzes te kunnen maken in een mogelijk aanbestedingstraject, heeft de gemeente besloten een marktconsultatie te organiseren. Op deze manier wil de gemeente een realistisch beeld krijgen van de mogelijkheden voor deze opdracht en er voor zorgen dat de proportionaliteit in de aanbesteding geborgd wordt. De uitkomst van deze marktconsultatie moet bijdragen aan het bepalen van een definitieve aanbestedingsstrategie en het vaststellen van een evenwichtig programma van eisen.

Graag nodigt de gemeente partijen uit die mogelijk geïnteresseerd zijn deel te nemen aan een toekomstige aanbesteding. Op voorhand spreekt de gemeente haar dank uit voor uw bereidheid om hieraan mee te werken. Vanzelfsprekend worden de beginselen van transparantie, gelijkheid en non-discriminatie bij deze marktconsultatie in acht genomen.

1.2. Korte beschrijving van de gemeente Bergen op Zoom

Bergen op Zoom is een gemeente met ca. 70.000 inwoners. De gemeente bestaat uit de kernen Bergen op Zoom, Halsteren, Heimolen, Kladde, Klutsdorp en Lepelstraat.

De organisatie van de gemeente Bergen op Zoom bestaat uit 15 afdelingen, waaronder Control & Audits, die opdrachtgever is voor deze marktconsultatie en mogelijke aanbesteding.

De vakgroep Aanbesteden & Contractmanagement zorgt voor procesbegeleiding.

Meer informatie over de gemeente Bergen op Zoom is te vinden op www.bergenopzoom.nl.

2. Beschrijving opdracht

Uitvoeren van de interne audit conform de ISO 27001 op basis van onderstaand auditplan

Inleiding

Dit auditplan is gebaseerd op de BIO2 handreiking voor het ISMS van de Informatiebeveiligingsdienst¹ en houdt rekening met de recente aanpassingen in de nummering en structuur van de ISO 27001 Annex A en ISO 27002. De audit wordt uitgevoerd over een periode van drie jaar, met jaarlijkse interne audits van het Information Security Management System (ISMS) van de gemeente Bergen op Zoom en een gefaseerde beoordeling van de geherstructureerde maatregelen uit de Annex A van ISO 27001 en ISO 27002 en de verplichte BIO2 overheidsmaatregelen. Dit plan zorgt ervoor dat alle vereiste maatregelen opzet, bestaan en werking van maatregelen worden beoordeeld. De resultaten van de interne audits zullen tevens dienen als input voor de management review en de verbetering van het ISMS.

Audit Doelstellingen

- **Jaarlijks:** Volledige interne audit van het ISMS om de continue naleving en verbetering van het beveiligingsbeheer te waarborgen.
- **Over 3 jaar:** Gefaseerde audit van de maatregelen in de nieuwe hoofdstukindeling van Annex A van ISO 27001/ISO 27002, waarbij elk jaar een deel van de maatregelen wordt beoordeeld op hun opzet, bestaan en werking
- **Scope:** De scope van de interne audit betreft de gedefinieerde kritieke processen² van de gemeente (Scope ISMS), focus van dit plan is het ISMS.
- **Management Review:** De bevindingen van de interne audits worden gebruikt voor de management review, met als doel om het ISMS te evalueren en waar nodig te verbeteren.

Jaar 1: ISMS Audit en Organisatorische Maatregelen (H5)

ISMS Audit

- **Scope:** Evaluatie van de algemene effectiviteit en naleving van het ISMS.
- **Focus:**
 - Risicobeoordeling en risicobeheerprocessen.
 - Beleid, procedures en verantwoordelijkheden.
 - Beheer van middelen en trainingsprogramma's.
 - Incidentbeheer en continue verbetering.

Audit van Organisatorische Maatregelen (H5, ISO27002)

- **Scope:** Controles die relevant zijn voor het beheer en de organisatie van informatiebeveiliging binnen de gemeente.
- **Maatregelen:**
 - Informatiebeveiligingsbeleid.
 - Toewijzing van verantwoordelijkheden.
 - Risicobeheerprocessen.
 - Beheer van externe partijen.
- **Auditdoelen:**
 - **Opzet:** Beoordeel of de organisatorische maatregelen effectief zijn ontworpen.
 - **Bestaan:** Verifieer of de maatregelen daadwerkelijk zijn geïmplementeerd.
 - **Werking:** Test of de maatregelen effectief functioneren zoals bedoeld.
- **Management Review:** De resultaten van deze audit zullen worden geëvalueerd tijdens de management review om verbeterpunten voor het ISMS te identificeren.

¹ <https://www.informatiebeveiligingsdienst.nl/product/bio2-handreiking-isms/>

² <https://www.informatiebeveiligingsdienst.nl/product/bio2-kritieke-processen-gemeenten/>

Jaar 2: ISMS Audit en Personele en Fysieke Maatregelen (H6 & H7 ISO 27002)

ISMS Audit

- **Scope:** Herbeoordeling van het ISMS met nadruk op wijzigingen en verbeteringen sinds de vorige audit.
- **Focus:**
 - Naleving van nieuwe of bijgewerkte regelgeving.
 - Evaluatie van geïdentificeerde zwakke punten en corrigerende maatregelen.
 - Veranderingen in het dreigingslandschap en de impact op risicobeheer.

Audit van Personele en Fysieke Maatregelen (H6 & H7)

- **Scope:** Controles gericht op personeelsbeheer en fysieke beveiligingsmaatregelen.
- **Maatregelen:**
 - **H6:**
 - Screening en werving van personeel.
 - Bewustwording en training.
 - Verantwoordelijkheden en beëindiging van contracten.
 - **H7:**
 - Beveiliging van faciliteiten.
 - Toegangsbeheer voor fysieke locaties.
 - Bescherming tegen omgevingsrisico's.
- **Auditdoelen:**
 - **Opzet:** Beoordeel of de personele en fysieke maatregelen effectief zijn ontworpen.
 - **Bestaan:** Verifieer of de maatregelen daadwerkelijk zijn geïmplementeerd.
 - **Werking:** Test of de maatregelen effectief functioneren zoals bedoeld.
- **Management Review:** De bevindingen van deze audit worden gebruikt om mogelijke verbeteringen voor het ISMS tijdens de management review te bespreken.

Jaar 3: ISMS Audit en Technische Maatregelen (H8)

ISMS Audit

- **Scope:** Eindbeoordeling van het ISMS voor de 3-jarige auditcyclus.
- **Focus:**
 - Evalueer de voortdurende effectiviteit van het ISMS en de naleving van ISO 27001.
 - Voorbereiding op de externe certificeringsaudit (indien van toepassing).
 - Analyse van de trends en lessen uit voorgaande audits.

Audit van Technische Maatregelen (H8)

- **Scope:** Beoordeling van technische beveiligingsmaatregelen en IT-processen.
- **Maatregelen:**
 - Toegangscontrole (IT-systemen).
 - Cryptografische technieken.
 - Netwerkbeveiliging.
 - Beheer van kwetsbaarheden en technische kwetsbaarheden.
 - Incidentdetectie en -respons.
- **Auditdoelen:**
 - **Opzet:** Beoordeel of de technische maatregelen geschikt zijn voor de dreigingen en risico's.
 - **Bestaan:** Verifieer of de technische maatregelen daadwerkelijk zijn geïmplementeerd.
 - **Werking:** Test of de technische maatregelen effectief functioneren zoals bedoeld.
- **Management Review:** De uitkomsten van deze audit zullen dienen als input voor de management review om eventuele aanpassingen en verbeteringen van het ISMS te overwegen.

Auditrapportage en Follow-up

- **Na elke audit:** Een gedetailleerd rapport met bevindingen, aanbevelingen en verbeterpunten.
- **Follow-up:** Na elke audit wordt een actieplan opgesteld om geïdentificeerde zwakke punten aan te pakken en de uitvoering van corrigerende maatregelen te waarborgen.
- **Jaarlijks overleg:** Bespreking van de auditresultaten met de CISO en relevante belanghebbenden, gevolgd door een herziening van het auditplan voor het volgende jaar indien nodig.
- **Management Review:** De resultaten van de interne audits worden jaarlijks geëvalueerd tijdens een management review, om de effectiviteit van het ISMS te waarborgen en om verbeteringen aan te brengen waar nodig.

Samenvattend

Dit driejarige ISMS-auditplan van de gemeente Bergen op Zoom biedt een systematische en grondige aanpak voor het waarborgen van de informatiebeveiliging binnen de organisatie volgens de nieuwe structuur van de ISO 27001/2-norm. Door jaarlijks het ISMS te auditen en de nieuwe hoofdstukken van Annex A over drie jaar te spreiden, wordt gezorgd voor een continue verbetering en naleving van de norm. De auditresultaten zullen dienen als cruciale input voor de management review, waardoor de organisatie in staat wordt gesteld om het ISMS voortdurend te evalueren en te verbeteren.

3. Voorwaarden tot deelname aan de marktconsultatie

Onderstaande tabel geeft een beschrijving van de algemene voorwaarden die de gemeente hanteert voor deelname aan de marktconsultatie. Deelnemers aan de marktconsultatie gaan onvoorwaardelijk akkoord met deze voorwaarden.

#	Voorwaarden
1	Partijen kunnen geen rechten ontleen aan de informatie die tijdens de marktconsultatie is verstrekt.
2	Tijdens de marktconsultatie verstrekte informatie kan afwijken van in de nog op te starten aanbestedings-procedure te verstrekken informatie.
3	Claims over het gebruik van informatie, vertrouwelijkheid of verzoeken om vergoedingen in verband hiermee worden niet gehonoreerd.
4	De gemeente is niet gebonden aan de uitkomsten van de marktconsultatie.
5	Er wordt geen vergoeding toegekend aan de deelnemers van deze marktconsultatie.
6	De aankondiging van deze marktconsultatie (incl. bijbehorende documenten), deelname of bijdrage aan de marktconsultatie gelden niet als uitnodiging tot inschrijving op de aanbesteding voor het onderhavige project, noch kunnen daaraan rechten worden ontleend.
7	De gemeente behoudt zich het recht voor de in dit document opgenomen plannings tussentijds te wijzigen.
8	De gemeente behoudt zich het recht voor om de marktconsultatie tijdelijk of definitief te staken.
9	De gemeente behoudt zich het recht voor naar aanleiding van deze marktconsultatie te besluiten (voorlopig) geen aanbesteding uit te voeren of de aanbesteding anders in te richten.
10	Deze marktconsultatie zal worden gevoerd in uitsluitend de Nederlandse taal.
11	De deelnemer aan de marktconsultatie draagt het risico van tijdige en volledige indiening van zijn vragen, antwoorden en aanvullingen binnen de marktconsultatie. De gemeente en TenderNed zijn niet verantwoordelijk voor fouten, die worden gemaakt door de deelnemers bij het aanleveren van informatie via de TenderNed software.

4. Marktconsultatie procedure

4.1. Planning

Datum	Omschrijving
14 augustus 2025	Publicatie marktconsultatiedocument middels een vooraankondiging via TenderNed
8 september 2025; 12.00 uur	Uiterste datum en tijdstip indienen vragen t.b.v. Nota van Inlichtingen
11 september 2025	Streefdatum verzending beantwoording Nota van Inlichtingen door de gemeente
25 september 2025; 12.00 uur	Uiterste datum en tijdstip indienen beantwoording marktconsultatievragen door deelnemers aan de marktconsultatie
2 oktober 2025	Consultatiegesprekken (<i>optioneel; datum onder voorbehoud van uitnodiging reserveren</i>)
31 oktober 2025	Geplande publicatie eindresultaat marktconsultatie

Deelnemers aan de marktconsultatie confirmeren zich expliciet aan bovenstaande systematiek van planning en doorlooptijd. Aan de planning kunnen geen rechten worden ontleend.

4.2. Communicatie tijdens de marktconsultatie

Alle communicatie over deze marktconsultatie verloopt digitaal via het TenderNed platform middels de Berichtenmodule.

Het is niet toegestaan om op een andere wijze contact te zoeken met medewerkers van de gemeente en met eventueel bij deze marktconsultatie betrokken externe adviseurs over deze aanbesteding, tenzij anders verwoord in deze marktconsultatie.

Het contact met u als inschrijver verloopt via één contactpersoon die uw organisatie vertegenwoordigt in deze marktconsultatie. De gegevens van deze contactpersoon dienen vermeld te worden bij de registratie in het TenderNed platform. De contactpersoon dient gemachtigd te zijn om namens de organisatie van de deelnemer aan de marktconsultatie te kunnen optreden en dient de Nederlandse taal in woord en geschrift in voldoende mate te beheersen.

4.3. Nota van inlichtingen marktconsultatie

De gemeente hanteert de volgende regels met betrekking tot de Nota van Inlichtingen:

- alle vragen met betrekking tot deze marktconsultatie dienen tijdig te worden aangeleverd met gebruik van **bijlage 1** Format Nota van Inlichtingen marktconsultatie dat u kunt aanleveren via de Berichtenmodule in TenderNed
- vragen die op een andere wijze worden gesteld, worden niet in behandeling genomen
- aan mondeling gedane uitspraken door of namens de gemeente inzake deze marktconsultatie kunnen geen rechten worden ontleend
- vragen kunnen doorlopend worden ingediend, de uiterste datum hiervoor is vermeld in de planning
- de gemeente kan vragen tussentijds beantwoorden, de streefdatum voor het beantwoorden van alle vragen is vermeld in de planning
- de antwoorden op de vragen maken integraal onderdeel uit van de marktconsultatie
- ingeval van tegenstrijdigheden tussen antwoorden in de Nota van Inlichtingen en de marktconsultatie, prevaleert hetgeen is bepaald in de antwoorden in de Nota van Inlichtingen
- de deelnemers die van oordeel zijn dat bepaalde informatie, vanwege het bedrijfsgevoelige karakter ervan, niet geschikt zijn voor verspreiding, dienen dit bij hun verzoek om inlichtingen kenbaar te maken

4.4. Consultatiegesprekken (optioneel)

Indien de gemeente, op basis van de beantwoording van de marktconsultatievragen, aanleiding ziet om verder met de betreffende deelnemer in gesprek te gaan, zal de gemeente deze deelnemer uitnodigen voor een consultatiegesprek. Het doel van deze gesprekken is om de gegeven antwoorden en de zienswijze van de deelnemer op het onderhavige onderwerp meer in detail te bespreken.

Deelnemers moeten bij hun beantwoording aangeven of zij eventueel wensen deel te nemen aan een dergelijk consultatiegesprek. Het initiatief hiertoe ligt uitsluitend bij de gemeente, deelnemers ontvangen hiervoor een uitnodiging. De datum waarop deze gesprekken plaatsvinden is reeds opgenomen in de planning. Deelnemers wordt verzocht hier rekening mee te houden.

De gesprekken zullen plaatsvinden in vergaderlocatie de Heerenkamer, Sint Annastraat te Bergen op Zoom. Voor ieder gesprek wordt maximaal 1 uur gereserveerd, waarbij de agenda als volgt is:

1. Voorstelronde incl. korte bedrijfsintroductie
2. Toelichting op verstrekte antwoorden door deelnemer en verdiepende vragen door gemeente
3. Tips, vragen en opmerkingen voor de gemeente

4.5. Eindverslag marktconsultatie

De resultaten van de marktconsultatie zal de gemeente Bergen op Zoom verwoorden in een samenvatting die als afronding van de marktconsultatie gepubliceerd wordt en tevens als bijlage bij de mogelijke aanbesteding wordt gevoegd. In het verslag worden de antwoorden op de door de gemeente gestelde vragen samengevat, rekening houdende met eventuele commerciële belangen van de marktpartijen. Indien een marktpartij van mening is dat bepaalde informatie uit haar beantwoording of een eventueel consultatiegesprek niet gedeeld mag worden in het eindverslag van de marktconsultatie, moet zij dit gemotiveerd aangeven. De gemeente beslist op basis van de motivatie of zij de economische belangen gerechtvaardigd vindt.

5. Vragenlijst marktconsultatie

Deze marktconsultatie bestaat uit vragen van de gemeente die in onderstaande tabel zijn weergegeven. De antwoorden op deze vragen kunt u invullen in **bijlage 2**, die vervolgens tijdig moet worden aangeleverd middels een bericht in de Berichtenmodule in TenderNed.

De antwoorden op de vragen worden doorgenomen door het projectteam van de gemeente.
Alle reacties worden met de grootst mogelijke zorgvuldigheid behandeld.

Nr.	Vraag
	Interne audit ISO 27001
1	Welke ervaring heeft u met het uitvoeren van interne audits op ISO 27001 bij een gemeente?
2	Kunt u aangeven op basis van de beoogde scope zoals beschreven in hoofdstuk 2 binnen welke bandbreedte de kosten op jaarbasis zouden liggen voor het uitvoeren van interne audits op ISO 27001?
3	De gemeente wil uiteraard naast de prijs ook kwalitatieve aspecten laten meewegen in de beoordeling van de offertes. Welke suggesties en/of aandachtspunten heeft u met betrekking tot de beoogde invulling van de kwalitatieve onderdelen van het gunningcriterium? Met andere woorden: op welke aspecten is de door u te leveren dienstverlening onderscheidend?
4	Kunt u aangeven of u wel of niet zou inschrijven op basis van de informatie uit deze marktconsultatie?
5	Kunt u suggesties geven op welke wijze de gemeente de inschrijfkans zou kunnen vergroten?
6	Welke trends en ontwikkelingen ziet u op het gebied van de beoogde scope binnen gemeenteland en hoe speelt u hierop in?
	Vervolg vraag uitbreiding scope naar certificering op ISO 27001
7	De gemeente onderzoekt de mogelijkheden en impact van een uitbreiding naar de certificering op ISO 27001. Welke ervaring heeft u daarmee en welke adviezen kunt u geven met betrekking tot certificering op ISO 27001?
8	Kunt u aangeven binnen welke bandbreedte de kosten op jaarbasis zouden liggen voor certificering op ISO 27001?
	Overig
9	Welke tips, informatie of adviezen wilt u de gemeente verder meegeven dat nog niet is behandeld in de bovenstaande vragen, maar naar uw mening wel van belang is voor het opstellen van een goede uitvraag?