

Verslag marktconsultatie

“Interne ISO 27001 audit”



1. Inleiding

De gemeente Bergen op Zoom heeft een marktconsultatie inzake 'Interne ISO 27001' georganiseerd. Doel van de marktconsultatie was om de markt te verkennen om tot inzichten, suggesties en ideeën te komen voor een actuele en marktconforme aanbesteding.

De gemeente heeft deze marktconsultatie via TenderNed nationaal gepubliceerd om de nationale markt zoveel mogelijk te bereiken en te betrekken. Vanzelfsprekend zijn de beginselen van transparantie, gelijkheid en non-discriminatie bij deze marktconsultatie in acht genomen. Er heeft een schriftelijke ronde plaatsgevonden in de vorm van een vragenlijst.

De gemeente bedankt alle deelnemers voor hun uitgebreide beantwoording en duidelijke toelichtingen.

Dit eindverslag van de marktconsultatie zal als bijlage bij de aanbestedingsstukken worden gevoegd, wanneer de gemeente besluit om tot een aanbestedingsprocedure over te gaan.

Het verslag is opgebouwd aan de hand van de schriftelijke ronde. De schriftelijke antwoorden zijn puntsgewijs in dit verslag opgenomen. Hierbij zijn de antwoorden (die mogelijk een bedrijfsgevoelig karakter zouden kunnen hebben) geanonimiseerd en op hoofdlijnen opgenomen.

2. Marktconsultatie

Interne ISO 27001 audit

Vraag 1

Welke ervaring heeft u met het uitvoeren van interne audits op ISO 27001 bij een gemeente?

- Een aantal deelnemers heeft inmiddels ervaring opgedaan met interne audits op ISO 27001 bij enkele gemeenten.
- Een aantal deelnemers heeft wel ervaring opgedaan binnen andere overheidsorganisaties maar (nog) niet veel bij gemeenten.
- Een enkele deelnemer heeft meer ervaring binnen het bedrijfsleven, maar nog niet binnen de gemeentelijke overheid.

Vraag 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?

- Uiteraard is een dergelijke inschatting volledig afhankelijk van de exacte scope van de opdracht.
- Gebaseerd op de informatie die gegeven is in de marktconsultatie lopen de inschattingen op jaarbasis uiteen van ca. € 2.000 tot ca. € 36.000.

Vraag 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?

- Er wordt een aantal aspecten genoemd. Met name voldoende ervaring met de specifieke gemeentelijke context kan bijdragen aan de kwaliteit, met uiteraard voldoende kennis van de relevante wet- en regelgeving.
- Ook wordt een aantal keren benoemd dat dergelijke audits niet alleen momentopnames zijn, maar dat een goede auditing partij zeker ook kan bijdragen aan continue verbetering binnen de organisatie.
- Rapportages gericht op verbetering en bestuurlijke besluitvorming wordt ook genoemd.

Vraag 4

Kunt u aangeven of u wel of niet zou inschrijven op basis van de informatie uit deze marktconsultatie?

- Op basis van de informatie die is gegeven in de marktconsultatie geven alle deelnemers aan naar verwachting wel te zullen inschrijven.
- Uiteraard is het heel belangrijk om de scope en reikwijdte van de opdracht goed te definiëren in de uitvraag met voldoende onderscheidend vermogen in de kwalitatieve subgunningcriteria.

Vraag 5

Kunt u suggesties geven op welke wijze de gemeente de inschrijfkans zou kunnen vergroten?

- De volgende aandachtspunten worden benoemd:
 - Stel een gedetailleerde uitvraag op met een duidelijke afbakening van de scope van de opdracht inclusief de doelstellingen die de gemeente wenst te behalen in welk tijdspad
 - Geef een duidelijk beeld van de huidige volwassenheid van de gemeentelijke organisatie
 - Biedt ruimte in de opdracht om naast de interne audit ook te adviseren en ondersteunen bij het opvolgen van verbeterpunten uit de interne audit

Vraag 6

Welke trends en ontwikkelingen ziet u op het gebied van de beoogde scope binnen gemeenteland en hoe speelt u hierop in?

- De Europese en nationale wetgeving (NIS2, Cyberbeveiligingswet, BIO2, ISO 27001) noodzaken gemeenten om hun informatiebeveiligingsmaatregelen steeds verder aan te scherpen.
- Ook is meer focus op beveiliging in de keten noodzakelijk, gemeenten worden steeds verder afhankelijk van externe leveranciers en cloudoplossingen; intensief contractbeheer en inzicht en controle op data-opslag en -verwerking worden steeds belangrijker.
- Daarnaast worden de ontwikkelingen met betrekking tot AI benoemd, wat enerzijds ten behoeve van verbetering van processen en dienstverlening kan worden ingezet, maar anderzijds ook continue gemonitord en gecontroleerd moet worden in het kader van risicobeheersing.

Vervolgvraag uitbreiding scope naar certificering op ISO 27001

Vraag 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?

- Er zijn nog niet veel gemeenten gecertificeerd op ISO 27001 binnen de ervaring van de deelnemers van deze marktconsultatie. Een enkele gemeente is zich op certificering aan het oriënteren.
- Als met het goed inrichten en uitvoeren van interne audits voldoende voorwerk is gedaan, kan certificering mogelijk nog maar een kleine stap zijn, maar de vraag is of het aantoonbaar voldoet aan de BIO of onderdelen daarvan mogelijk waardevoller kan zijn dan certificering.
- Met certificering op informatiebeveiliging kan de gemeente wel aantonen aan haar burgers, samenwerkingspartners en ander stakeholders dat zij een betrouwbare partij is.
- Er lijkt een verschuiving plaats te vinden van compliant werken naar een meer risico-gebaseerde aanpak. Het gaat meer om structurele identificatie, beoordeling en beheersing van risico's.
- Belangrijk is wel om eerst het ISMS binnen de organisatie goed en effectief te laten functioneren, alvorens verder te kijken naar mogelijke certificering.
- Intern draagvlak is van belang, alsook de bewustwording en training van medewerkers op het vlak van informatiebeveiliging.

Vraag 8

Kunt u aangeven binnen welke bandbreedte de kosten op jaarbasis zouden liggen voor certificering op ISO 27001?

- Niet alle deelnemers hebben hier een inschatting van gegeven.
- Inschattingen van de kosten zijn op basis van de nu bekende informatie niet goed te maken, maar lopen uiteen van ca. € 10.000 tot € 50.000 op jaarbasis, eenmalige kosten bij implementatie niet meegerekend.

Overig

Vraag 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?

- Enkele suggesties die worden genoemd zijn:
 - Duidelijke afbakening van de scope en doelstellingen, zowel voor de interne audit als voor mogelijke wensen voor aansluitende certificering
 - Goede samenwerking en kennisoverdracht kan bijdragen aan continue verbetering

3. Tot slot

- Deelnemende partijen kunnen geen rechten ontlelen aan de informatie die tijdens de marktconsultatie is verstrekt.
- Tijdens de marktconsultatie verstrekte informatie kan afwijken van in de nog op te starten aanbestedingsprocedure te verstrekken informatie.
- Claims over het gebruik van informatie, vertrouwelijkheid of verzoeken om vergoedingen in verband hiermee worden niet gehonoreerd.
- De gemeente is niet gebonden aan de uitkomsten van deze marktconsultatie.
- Er wordt geen vergoeding toegekend aan de deelnemers van deze marktconsultatie.
- De aankondiging van deze marktconsultatie (incl. bijbehorende documenten), deelname of bijdrage aan de marktconsultatie gelden niet als uitnodiging tot inschrijving op de aanbesteding voor de onderhavige opdracht, noch kunnen daaraan rechten worden ontleend.