

Marktconsultatie Implementatie ISO27001

Uitgevoerd door : Het NIC B.V., Joost van den Bekerom
In opdracht van : Provincie Zeeland, Middelburg
Datum : 11 december 2017



Inhoudsopgave

1.	Inleiding.....	3
1.1	Beschrijving van de aanbestedende dienst	3
1.2	Aanleiding aanbesteding	3
1.3	Doel van de marktconsultatie	4
2.	Procedure.....	6
2.1	Publicatie	6
2.2	Openbaarheid resultaten.....	6
2.3	Uitvoering marktconsultatie	6
2.4	Gelegenheid tot het stellen van vragen en nota van inlichtingen	6
2.5	Planning	7
2.6	Voorwaarden	7
3.	Vragen marktconsultatie	8
	Bijlagen	10

1. Inleiding

1.1 Beschrijving van de aanbestedende dienst

De aanbestedende dienst is de Provincie Zeeland. We leven in een snel veranderende samenleving en van de provincie wordt verwacht dat wij flexibel, creatief en innovatief zijn en dat onze organisatie maatschappelijke opgaven snel, klantvriendelijk en adequaat aanpakken. Dit betekent dat wij een wendbare organisatie moeten zijn die snel en slagvaardig kan inspelen op een veranderde vraag. De provinciale organisatie wijzigt continu en vanuit organisatieontwikkeling wordt meer en meer ingestoken op een organisatie die werkt met opgaven, programma's en projecten en steeds minder met hiërarchische structuren (van lijnorganisatie naar matrixorganisatie).

Politiek bestuurlijke organisatie

De Provinciale Staten (PS) van Provincie Zeeland zijn het aanbestedende orgaan. Voor het dagelijks bestuur is het College van Gedeputeerde Staten (GS) verantwoordelijk.

Ambtelijke organisatie

De provinciale organisatie bestaat uit de directie en verschillende afdelingen. Naast de afdelingen bestaat er een concernstaf en kabinet. De leiding van de provinciale organisatie is in handen van de directie. Daarnaast is er de door de werkgeverscommissie van Provinciale Staten aangestuurde statengriffie en de onafhankelijke Rekenkamer Zeeland.

Meer informatie betreffende de organisatie van Provincie Zeeland kunt u vinden op de website www.zeeland.nl.

1.2 Aanleiding aanbesteding

Informatie is één van de voornaamste bedrijfsmiddelen van de Provincie Zeeland. Het verlies van gegevens uitval van ICT, of het door onbevoegden kennismaken of manipuleren van bepaalde informatie, kan gevolgen hebben voor de bedrijfsvoering, maar kan ook leiden tot imagoschade, politieke consequenties, economische schade of zelfs in de meest extreme situatie dodelijke ongevallen. De Provincie is verantwoordelijk voor de informatie die zij verwerkt en moet hier zorgvuldig en veilig mee omgaan.

De Provincie heeft een omvangrijk takenpakket waarbij de te leveren producten en diensten worden ondersteund door een uitgebreid scala aan informatiesystemen, datasystemen en softwaretoepassingen, ook van externe ketenpartner. Zie bijlage 1 voor het huidige applicatielandschap.

In 2013 is de werkgroep Informatiebeveiliging opgericht met als doel om een informatieveilige organisatie te creëren. De werkgroep is voor de hele organisatie het belangrijkste aanspreekpunt voor zaken die te maken hebben met de veiligheid van informatie. De werkgroep is betrokken bij alle inspanningen die bijdragen aan een betrouwbare informatievoorziening en bewaken de gestelde kaders op het gebied van betrouwbaarheid, beschikbaarheid en integriteit van informatie. Verder zijn ze verantwoordelijk voor de uitwerking en implementatie van de strategie en het beleid gericht op informatiebeveiliging. Er is in de huidige structuur voor gekozen om niet één CISO-functie aan te stellen, maar deze taken te verdelen over meerdere personen binnen de werkgroep. Zie bijlage 2 voor de huidige werkgroepstructuur.

Om de processen rondom informatiebeveiliging binnen 4 jaar naar een hoger niveau te brengen is er het volgende doel voor ogen:

In 2021 provinciebreed op alle vlakken rondom informatiebeveiliging gereed te zijn voor ISO27001 certificering. Dit in lijn met de interprovinciale afspraken om langs de lijnen beschikbaarheid, vertrouwelijkheid en integriteit verbetermaatregelen door te voeren.

Onlangs is er een impactanalyse voor informatiebeveiliging gemaakt welke inzicht geeft in wat er allemaal moet worden geregeld om ISO 27001 gecertificeerd te kunnen zijn. Zie bijlage 3 voor het document. Op dit moment ontbreekt het in de werkgroep aan voldoende expertise om dit doel te bereiken.

Stand van zaken tot nu toe

Tot op heden is veel werk verricht op het gebied van implementeren van beheersmaatregelen conform ISO 27002. De Plan-do-Check-Act kant op basis van ISO 27001 is tot nu toe onderbelicht geweest.

Vanaf 2014 is de werkgroep aan de slag om de informatieveiligheid provinciebreed te borgen en een veiligheidsniveau te hanteren om ongewenste verspreiding van vertrouwelijke informatie en ongewenste toegang tot de Provincie te voorkomen.

In 2015 is het beleidskader informatiebeveiliging geactualiseerd en vastgesteld. In dit jaar heeft de focus vooral gelegen op de technische beveiliging en in beeld brengen van de architectuur. Er zijn ook een aantal processen en beleidsrichtlijnen uitgewerkt en geïmplementeerd, bijvoorbeeld beleid voor ICT toegang, cloud- en webapplicaties en beheerprocessen I&A.

In 2016 is bij Provincie Zeeland gewerkt aan het optimaliseren, toetsen en verder uitwerken van het informatiebeveiligingsbeleid. De belangrijkste aspecten daarbij zijn: het implementeren van diverse technische beheersmaatregelen, bewustwording bij de medewerkers en het opstellen van beleidsrichtlijnen. Ook is in dit kader een proces ingeregeld met betrekking tot de Wet bescherming persoonsgegevens ("Meldplicht Datalekken"). In de tweede helft van 2016 is een 1-meting uitgevoerd door interne medewerkers van Provincie Zeeland. Eind 2016 heeft een interne training plaatsgevonden voor de implementatie van de algemene ISO27001/2 norm.

Begin 2017 is gestart met de implementatie van diverse beveiligingsrichtlijnen voor wijzigingsbeheer, logische toegangsbeveiligingsbeleid en wachtbeleid en het verder aanscherpen van de IT beveiliging. Verder zijn diverse acties ondernomen voor bewustwording en implementatie van de Europese privacywetgeving. In september 2017 zijn er een aantal bijeenkomsten georganiseerd om de bewustwording rondom informatiebeveiliging te vergroten bij GS, Directie, PS en medewerkers. Verder is een impactanalyse uitgevoerd voor wat betreft de implementatie van de Algemene Verordening Gegevensbescherming (AVG).

1.3 Doel van de marktconsultatie

Het doel van deze marktconsultatie is om, voorafgaand aan het formele aanbestedingsproces, vrijblijvend en openbaar informatie te verkrijgen vanuit de markt wat betreft de omvang en opdrachtwaarde. De verkregen informatie zal onder meer gebruikt worden om kwalitatief de opdracht beter te kunnen specificeren en om de keuze van de aanbestedingsvorm te bepalen. Op deze wijze

kan de aan te besteden opdracht afgestemd worden op de mogelijkheden die er zijn in de huidige markt.

De Provincie zoekt een senior adviseur/begeleider van een ter zake kundige externe partij die de werkgroep Informatiebeveiliging begeleidt en ondersteunt bij het bereiken van deze doelstelling. In de uitvoering van deze werkzaamheden dient – voor zover mogelijk - ook een koppeling te worden gelegd met het provinciale informatiebeleid, reeds ontwikkelde en geïmplementeerde beleidsrichtlijnen en de daaraan gerelateerde procedures en architectuurprincipes.

Voor de omvang van de opdracht wordt vooralsnog uitgegaan van 4 dagen per maand, waarvan 2 dagen op locatie Provinciehuis Zeeland in Middelburg. De continuïteit van de dienstverlening dient zodanig te worden geborgd dat in geval van langdurige ziekte/verhinderings een collega-senior adviseur/begeleider uiterlijk binnen 5 werkdagen deze taken probleemloos zonder kwaliteitsverlies kan overnemen.

De taken zijn als volgt:

- Projectleiding en -vormgeving provinciebrede implementatie ISO 27001 (gereed maken voor certificering eind 2021);
- Omvormen acties uit de interprovinciale nulmeting en de impactanalyse tot werkpakketten en advies geven over prioritering;
- Opstellen provinciebrede plan van aanpak n.a.v. impactanalyse en eigen ISO-27001 implementatie-ervaring;
- Aanreiken, op maat snijden en implementeren van best practice instrumenten, bijv. een tool voor het bewaken van de voortgang PDCA cyclus (ISMS), een sjabloon voor het uitvoeren van impact- en dreigingenanalyses, voorbeelduitwerkingen beleidsrichtlijnen;
- Adviseren over rollen/verantwoordelijkheden informatiebeveiliging vanaf 2019 incl. afweging of CISO nodig is en uitwerken van taken en rollen van de werkgroep inclusief het juridische vakgebied;
- Kennis en ervaring van de werkgroepleden, management en bestuur op peil brengen voor wat betreft ISO 27001/2.

Competenties externe senior adviseur/begeleider ISO 2001 certificeringstraject

- Academisch werk- en denkniveau, aangevuld met projectmanagement specifieke certificeringen;
- Minimaal 3 jaar relevante werkervaring als senior projectmanager;
- Meerjarige ervaring met risicomanagement en verandermanagement;
- Meerjarige ervaring met het begeleiden van ISO-27001 certificeringstrajecten in complexe organisaties;
- Meerjarige ervaring met het adviseren in bestuurlijke en politiek gevoelige organisaties;
- Vaardigheid in het ontwikkelen, uitdragen en verdedigen van adviesinstrumenten;
- Goede communicatieve vaardigheden, zowel mondeling als schriftelijk;
- Goed kunnen samenwerken met verschillende disciplines op verschillende niveaus;
- Integer, overtuigingskracht en resultaatgericht;
- Kennis van de actuele stand van zaken en mogelijkheden van ICT, ontwikkel en beheermethoden;
- Specifieke certificeringen rondom ISO 27001/2 en IT-audits.

2. Procedure

In dit hoofdstuk is de procedure beschreven. Deelneming aan de marktconsultatie dient conform de aanwijzingen in dit hoofdstuk gedaan te worden.

2.1 Publicatie

Provincie Zeeland heeft er voor gekozen om deze marktconsultatie in breed verband uit te voeren, teneinde alle potentieel geïnteresseerde marktpartijen in de gelegenheid te stellen aan dit proces deel te nemen. Om deze reden is de marktconsultatie gepubliceerd op TenderNed.

2.2 Openbaarheid resultaten

De Provincie Zeeland streeft er naar dat bij de aanbesteding van de opdracht alle potentiële inschrijvers gelijk geïnformeerd worden en zal een geanonimiseerd resumé van de resultaten van de marktconsultatie beschikbaar stellen aan de deelnemers. Bij een mogelijke aanbesteding die voortkomt uit deze marktconsultatie zal de uitkomst (geanonimiseerd) ook worden bijgevoegd bij de desbetreffende aanbestedingsdocumenten.

Indien een deelnemer aan de onderhavige marktconsultatie acht dat gegeven informatie concurrentiegevoelige informatie is, dan kan dit door de deelnemer worden aangegeven. De Provincie zal in voorkomend geval deze informatie dan niet openbaar maken.

2.3 Uitvoering marktconsultatie

Geïnteresseerde marktpartijen worden uitgenodigd om de in hoofdstuk 3 opgenomen vragen te beantwoorden en uiterlijk in te dienen op **maandag 15 januari 2018 14:00**. Wij verzoeken u om voor de beantwoording gebruik te maken van het bijgevoegde antwoordformulier (bijlage 4).

Gelieve bij de beantwoording de volgorde van de vragenlijst aan te houden.

Bovengenoemde datum en tijdstip zijn een fataal moment. TenderNed sluit op aangegeven moment de kluis, op dat moment dient het gehele inschrijfproces in TenderNed te zijn afgerond.

2.4 Gelegenheid tot het stellen van vragen en nota van inlichtingen

De deelnemers kunnen, uitsluitend via de vraag en antwoorden module tot en met **maandag 18 december 2017 14.00** inhoudelijke vragen stellen via TenderNed. Van deze vragen met de bijbehorende antwoorden wordt een geanonimiseerde nota van inlichtingen opgesteld.

Wij beseffen dat er nog details in de aangereikte informatie ontbreken omdat de documenten nog globale beschrijvingen bevatten. Aangezien momenteel de informatie nog niet compleet is, zal het niet in alle gevallen mogelijk zijn om detailvragen te beantwoorden. Van de deelnemers wordt verwacht dat zij bij de opstelling van de eventuele vragen hiermee rekening houden.

Eventuele technische vragen over het systeem, kunt u rechtstreeks stellen bij TenderNed, zie onderstaand.

TenderNed	Voor technische vragen over het aanbestedingsplatform		
Contactpersoon	Servicedesk van TenderNed		
Telefoonnummer	0800 8363 376	Mailadres	Servicedesk@TenderNed.nl

Adviesbureau	Het NIC		
Procesbegeleider	Joost van den Bekerom	Functie	Consultant
Telefoonnummer	06 30 72 61 43	Berichten: via de berichtenmodule op het aanbestedingsplatform TenderNed	

2.5 Planning

Maandag 11 december 2017	Publicatie Aankondiging van een schriftelijke marktconsultatie t.b.v. TenderNed
18 december 2017 14:00 uur	Sluiting termijn voor het indienen van vragen met betrekking tot dit marktconsultatie document
21 december 2017	Streefdatum beschikbaarstelling Nota van Inlichtingen
Maandag 15 januari 2018 14:00 uur	Sluiting van marktconsultatie t.b.v. TenderNed
Maandag 22 januari 2018	Publicatie schriftelijke rapportage van marktconsultatie t.b.v. TenderNed aan alle deelnemende marktpartijen

2.6 Voorwaarden

- Deelname aan de marktconsultatie is geheel vrijwillig en vrijblijvend en heeft op geen enkele wijze gevolgen voor een eventuele deelname aan de aanbesteding die zal worden gestart. Partijen kunnen geen aanspraak maken op vergoedingen van eventueel gemaakte kosten in het kader van de marktconsultatie.
- Het consultatiedocument is slechts geschreven in het kader van de marktconsultatie voor deze aanbesteding. De marktconsultatie is geen uitnodiging om in te schrijven op de aanbesteding, waarvoor deze marktconsultatie als voorbereiding dient.
- De aanbestedende dienst behoudt zich het recht voor om het traject van de marktconsultatie en/of de aanbestedingsprocedure geheel of gedeeltelijk te staken.
- Er kunnen op geen enkele wijze rechten worden ontleend aan de ten behoeve van de marktconsultatie verstrekte informatie. Dit geldt zowel voor de aanbestedende dienst als voor de marktpartij.
- Door deelname aan de marktconsultatie verklaart de deelnemende marktpartij akkoord te zijn met alle genoemde voorwaarden.
- De door middel van deze marktconsultatie aan Provincie Zeeland verstrekte informatie wordt vertrouwelijk behandeld en wordt niet gebruikt voor een ander doel dan het opdoen van marktkennis teneinde tot een kwalitatief betere aanbesteding te komen.

3. Vragen marktconsultatie

Onderstaand en in bijlage 4 vindt u de door ons geformuleerde vragen voor deze marktconsultatie. Wij vragen u deze te beantwoorden middels het geheel invullen van de bijlage en in te dienen onder het tabblad 'Documenten' in TenderNed.

De vragen zijn opgesteld aan de hand van de in paragraaf 1.2 beschreven aanleiding van de aanbesteding en in paragraaf 1.3 beschreven doelstelling van de marktconsultatie. Wij willen u vragen om bij de beantwoording van de vragen hiermee rekening te houden.

1. Is de scope van de opdracht zoals beschreven in paragraaf 1.3 (doel van de marktconsultatie) voldoende duidelijk? Zo nee, kunt u aangeven op welke punten onduidelijkheden en onvolkomenheden zijn en hoe zouden we dit beter kunnen verwoorden?
2. Kunt u zich vinden in de voorgestelde omvang van de opdracht (4 dagen per maand, waarvan 2 dagen op locatie Provinciehuis Zeeland in Middelburg. De continuïteit van de dienstverlening dient zodanig te worden geborgd dat in geval van langdurige ziekte/verhinderings een collega-senior adviseur/begeleider uiterlijk binnen 5 werkdagen deze taken probleemloos zonder kwaliteitsverlies kan overnemen)?
 - a) Zo ja, welke prijsstelling (opdrachtraming) is realistisch?
 - b) Zo nee, welke omvang denkt u zelf aan en welke opdrachtraming is vervolgens realistisch?
3. Is het haalbaar om in 2021 ISO27001 gecertificeerd te zijn, vooral met oog op het complexe applicatielandschap (bijlage 1) en de complexe ambtelijke, bestuurlijke en politieke organisatie?
4. Er is een werkgroep informatiebeveiliging, bestaande uit 9 mensen (zie bijlage 2). Welke rol- en taakverdeling ziet u voor deze werkgroep nu (2018) en in de toekomst (vanaf 2019) om toe te kunnen werken naar de ISO 27001 certificering? Welke expertises, personen en capaciteitsinzet verwacht u in de werkgroep?
5. In hoeverre is een resultaatsverplichting mogelijk om in 2021 ISO27001 provinciebreed gecertificeerd te zijn? Welke voorwaarden ziet u in dit kader? Wat is een realistische prijsstelling? Wat betekent dit voor uw dienstverlening in het kader van samenwerking versus medewerking?
6. Welke tools kunt u inzetten en op maat snijden voor rapportage- en meetdoeleinden en/of sjablonen voor uitvoeren risicoanalyses, PDCA etc.? Wat is een realistische prijsstelling? In hoeverre kan de Provincie Zeeland hier licentievrij gebruik van (blijven) maken?
7. Op welke manier kan de kennis en ervaring van de werkgroepleden, management en bestuur op peil worden gebracht? Hoe kan er draagvlak bij management en bestuur worden gecreëerd? Welke gevolgen heeft dit opleidingsdeel/ambassadeursdeel voor de prijsstelling?
8. Welke risico's ziet u in deze opdracht, gelet op een organisatie als de Provincie Zeeland? En welke maatregelen adviseert u om deze risico's te minimaliseren?

9. In welke mate is bestendiging van het informatiebeveiligingsniveau noodzakelijk (terugkerende audits, terugkerende bewustwordingssessies, sessies voor functioneel applicatiebeheerder, etc.)? En wat doet dit in de prijsstelling? Is hier een abonnementsvorm mogelijk?
10. In hoeverre is een interne auditor noodzakelijk en welke acties/expertise/werkervaring/opleidingen zijn hiervoor nodig? Wat is de prijsstelling om dit te realiseren?
11. Zie bijlage 3 paragraaf 7.2 voor competenties. In hoeverre zijn deze realistisch? Zijn hier aanvullingen of opmerkingen op? Wat is de prijsstelling om deze mensen op te leiden?
12. Kunt u inzicht geven in de kosten voor een externe audit aan het eind van het traject, om ISO27001 gecertificeerd te raken?
13. Hoe ziet u de samenwerking met de accountant? Hoe kan de accountant overtuigd raken van en betrokken blijven bij het informatiebeveiligingsbeleid? Welke rol ziet u hierin voor uzelf en voor de accountant?
14. We overwegen om een aantal extra taken mee te nemen in de aanbesteding (2 dagen extra per maand). Dit betreft taken rondom het implementeren van beveiligingsmaatregelen conform de ISO 27002 op locatie Provinciehuis Zeeland in Middelburg. De belangrijkste werkzaamheden zijn:
 - Coördineren van complexe implementatietrajecten rondom de te nemen beveiligingsmaatregelen;
 - Het overdragen van kennis en ervaring aan de werkgroepleden voor wat betreft het uitvoeren van impact- en dreigingenanalyses en het implementeren van ISO 27002 maatregelen;
 - Ontwikkelen van beveiligingsrichtlijnen- en maatregelen volgens de ISO 27002;
 - Zorg dragen voor documentatie van de beveiligingsmaatregelen en hierover rapporteren aan de werkgroep informatiebeveiliging.

We denken aan het volgende competentieprofiel:

- Academisch werk- en denkniveau;
- Kennis en ervaring op het gebied van projectmatig werken en adviseren;
- Kennis en ervaring op het gebied van informatiebeveiliging en risicoanalyse methoden;
- Kennis van de actuele stand van zaken en mogelijkheden van ICT;
- Kennis van de ISO 27001/27002 normen;
- Initiatiefrijk, resultaatgericht en flexibel;
- Integer;
- Overtuigingskracht;
- Goede communicatieve vaardigheden, zowel mondeling als schriftelijk;
- Goed kunnen samenwerken met verschillende disciplines op verschillende niveaus.

- a) Kunt u vinden in het geschetste profiel en heeft u hierover nog opmerkingen/aanvullingen?
- b) Welke prijsstelling (opdrachtraming) is realistisch?

Bijlagen

Bijlage 1. Applicatielandschap

Bijlage 2. Werkgroepstructuur Informatiebeveiliging 2018

Bijlage 3. Impactanalyse Informatiebeveiliging voor ISO 27001 certificering

Bijlage 4. Antwoordformulier