

AANBESTEDING GRC

BIJLAGE 01 OPDRACHTOMSCHRIJVING GOVERNANCE RISK EN COMPLIANCY TOOL MET AUDITFUNCTIONALITEIT



1 INHOUDSOPGAVE

1	INHOUDSOPGAVE	2
2	DOEL VAN GRC-TOOL	3
2.1	Doelstelling ICT-Oplossing.....	3
2.2	Doelstellingen van deze aanbesteding	3
3	HUIDIGE SITUATIE.....	4
4	GEWENSTE SITUATIE	5
4.1	Algemeen	5
4.2	Procesbeschrijving.....	6
5	AANTALLEN	7
5.1	Informatiebeheer	7
5.2	Security	7
5.3	Audit & Control	7
5.4	Privacy.....	7
6	ARCHITECTUUR	8
6.1	Referentie-architectuur.....	8
7	SCOPE VAN DE OPDRACHT	9
8	CRITERIA.....	9
9	MARKTVERKENNING.....	9
10	SAMENWERKING MET GEMEENTE GRONINGEN.....	10
10.1	Implementatie	10
10.2	Exploitatie	10
11	SAMENWERKING MET SOFTWARE INTEGRATOR.....	10
12	TIJDLIJNEN	10
12.1	Aanbestedingsfase	10
12.2	Contract- en verificatiefase	10
12.3	Vorbereiding implementatie.....	10
12.4	Implementatiefase	11
12.5	Beheerfase	11
13	ORGANOGRAM GEMEENTE GRONINGEN	12

2 DOEL VAN GRC-TOOL

De gemeente Groningen beoogt GRC- tool met auditfunctionaliteit (ICT-oplossing) aan te schaffen om:

- Systematisch governance processen te beheren, risicobeoordelingen uit te voeren en naleving van regelgeving te waarborgen. De software helpt ons processen te centraliseren en automatiseren waardoor we efficiënter kunnen werken en een beter overzicht krijgen van de risico's en naleving van wet- en regelgeving.
- Te ondersteunen bij de planning, uitvoering, voortgangs- en kwaliteitsbewaking van de interne audits waarbij wordt voldaan aan de controlestandaarden van NBA en IIA. De aan te schaffen tooling moet zo mogelijk voorzien in ondersteuning bij de planning, uitvoering en rapportage van specifieke adviesopdrachten en themaonderzoeken naar deelelementen van interne sturing, beheersing en (financiële) verantwoording.
- Te ondersteunen bij het opstellen en bijhouden van het verwerkingsregister en nalevingsbeheer van privacywetgeving.
- Zorg te dragen voor een verbeterde ondersteuning van de kwaliteitssystematiek (of interne beheersing) in de gemeente Groningen voor informatiebeheer en security, alsmede het uitvoeren van toezicht vanuit Privacy en de onafhankelijke en objectieve toetsing (van governance, risk en compliance) door Audit.

Ambtelijk en bestuurlijk verantwoordelijken worden hiermee in staat gesteld verantwoording af te leggen over de mate van naleving van hun eigen beleid en of vigerende wet- en regelgeving en daardoor in staat gesteld om daarin verbeteringen door te voeren.

2.1 DOELSTELLING ICT-OPLOSSING

- Verbeterde Governance, versterken van de bestuurlijke processen binnen de gemeente Groningen;
- Risicobeheer, identificeren, evalueren en beheren van risico's binnen de gemeente Groningen;
- Compliance, Waarborgen dat de gemeente Groningen voldoet aan de relevante wet- en regelgeving.
- Transparantie en verantwoording, het mogelijk maken van gedetailleerde en gemeentebrede rapportages, audit-trails en controlemechanismen om de besluitvorming en algehele prestaties te kunnen verbeteren;
- Veiligheid van gegevens, voldoen aan de Privacywetgeving, AVG en WPG (Wet PolitieGegevens)
- Vergroten van effectiviteit en efficiëntie van de evaluatie/controle van de processen van Governance, Risk en Compliance door de 1^e, 2^{de} en 3^{de} lijn (3LOD) en de samenwerking tussen de verschillende lijnen.
- Het ondersteunen in het op orde brengen en houden van het gemeentelijk Informatiebeheer
- Een meer intuïtief, moderner en gebruiksvriendelijk tool voor (eind) gebruikers.

2.2 DOELSTELLINGEN VAN DEZE AANBESTEDING

Standaardisatie van de werkwijze rondom de GRC (Governance, Risico's en Compliance) processen alsmede de onafhankelijke toetsing daarvan, voor organisatieonderdelen binnen de gemeente Groningen die (toekomstig) gaan aansluiten.

Doelstellingen relevant voor deze aanbesteding:

- Verwerven van de meest geschikte leverancier;
 - Best passend bij de gemeente Groningen
 - Ervaring passend bij de behoefte en wensen van de gemeente Groningen;
- Selecteren en langdurig gebruiken van de (best passende) geïntegreerde oplossing
 - Meest standaard out-of-the-box (SaaS) oplossing voor de bedrijfsprocessen;
 - Geen maatwerk, wel gebruik van best practices

- Eén geïntegreerd platform voor de gehele organisatie met betrekking tot interne (proces)beheersing voor 1^e en 2^e en 3^{de} lijn;
- Verhogen van de operationele efficiëntie;
 - Door goede afbakening van 1^e lijns-beheer door gemeente Groningen en 2^e (en 3^e) lijns Beheer door de Leverancier in het kader van ITSM;
 - Flexibiliteit in noodzakelijke (tool) aanpassingen bij voortschrijdend inzicht en wetgeving;
- Naleving wet- en regelgeving;
 - Europese aanbestedingswet;
 - Wat betreft relevante wet- en regelgeving met betrekking tot toezicht op de uitvoering van bedrijfsvoering gemeente Groningen waaronder tenminste de Privacywetgeving, AVG en WPG (Wet Politie Gegevens)
 - Frameworks en normenkaders; de VNG-handreiking Verantwoording Archiefwet via Kritische Prestatie Indicatoren (KPI's), Kwaliteitssysteem Informatiebeheer Decentrale Overheden (KIDO), ENSIA, BIO, ISO27001 en ISO27002 en het privacy normenkader van VNG realisatie.
- Maatschappelijke doelstelling gemeente Groningen;
 - Bij deze aanbesteding beogen wij de maatschappelijke doelstelling in te kunnen vullen door middel van 'Social Impact'.

3 HUIDIGE SITUATIE

In 2018 is het kwaliteitssysteem informatiebeheer van de gemeente Groningen geschreven. Bij de implementatie van dit kwaliteitssysteem is de systematiek niet volledig geïmplementeerd. Bij de uitvoering en monitoring is geconstateerd dat het huidige kwaliteitssysteem op een aantal punten niet of onvoldoende voldoet. Het proces is vooral een handmatig en arbeidsintensief proces, waarbij er een gebrek is aan (tussentijdse) monitoring en eenduidige rapportagemogelijkheden.

Het kwaliteitssysteem wordt op dit moment ook niet ondersteund door een kwaliteitsmanagement-programmatuur die de aandachtsgebieden bewaakt rondom Governance, Risico's en Compliance (GRC).

Na inventarisatie van de behoefte van Informatiebeheer is er een bredere inventarisatie gedaan bij andere organisatieonderdelen die een vergelijkbare behoefte en werkproces hanteren binnen de gemeente Groningen.

De gemeente Groningen heeft op dit moment niet de beschikking over ondersteunende software die organisatie breed ingezet kan worden voor Governance, Compliance & Risk processen in de eerste en tweede lijn binnen en het onafhankelijk toetsen hiervan binnen de derde lijn..

Het volgende kan worden vastgesteld over de huidige situatie:

- Er is binnen de gemeente Groningen geen integrale werkwijze met betrekking tot het beoordelen van de kwaliteit van informatie en processen;
- Organiseatieonderdelen hanteren afzonderlijk van elkaar een eigen werkwijze voor het beoordelen van de kwaliteit, processen, risico's en verbeteringen;
- Er bestaat een bredere behoefte voor een ICT-oplossing en een generiek gebruik ervan binnen de gemeente Groningen;
- Er bestaat een behoefte vanuit Auditing om aan te sluiten bij de GRC wanneer deze een passende auditmanagement functionaliteit biedt.
- De gemeente Groningen heeft uitgesproken een generieke tool voor de GRC-processen en de evaluatie van deze GRC-processen te willen implementeren
- We beseffen ons dat nog niet alle organisatieonderdelen al even enthousiast zijn voor het (verplicht) gebruiken van de ICT-oplossing waardoor de implementatie naar verwachting wat extra aandacht nodig zal hebben.

4 GEWENSTE SITUATIE

4.1 ALGEMEEN

Vanuit wet- en regelgeving (en de interne eisen en wensen) worden er meer eisen gesteld aan de wijze waarop de kwaliteit van informatie en processen wordt vastgesteld, controles worden uitgevoerd en hoe er gerapporteerd wordt over het bestaan, de werking, de kwaliteit en de eventuele verbeterpunten die meegenomen kunnen worden bij de uitvoering.

Er is een organisatie-brede behoefte om een uniforme werkwijze te hanteren op het gebied van kwaliteit (Governance, Risico's, Compliance).

Door het toepassen en gebruiken van de ICT-oplossing, kan gemeente Groningen een standaard werkwijze inrichten om in control te komen van het beheren van informatie en processen en de evaluatie hiervan door de derde lijn. Dit kan (moet) ook gaan gelden als leidraad voor organisatieonderdelen die op dit moment een latente behoefte hebben voor een ICT-oplossing. Deze organisatieonderdelen kunnen in de toekomst aansluiten (en gebruikmaken) van de al opgedane kennis die is opgedaan met de uiteindelijke inrichting van de ICT-oplossing.

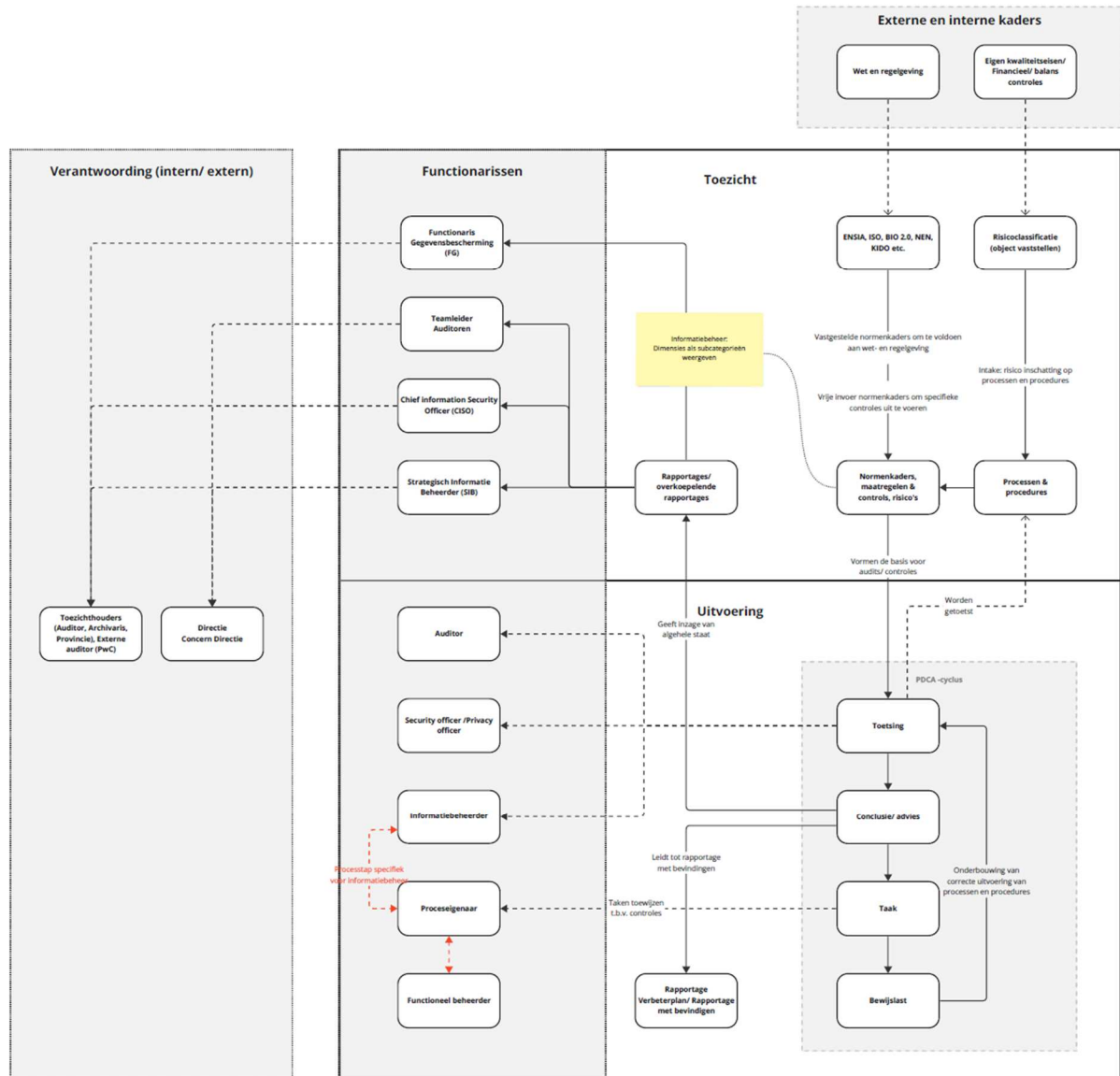
In de ideale situatie heeft de gemeente Groningen één tool in huis waarmee alle GRC-processen binnen de gehele gemeente Groningen worden ondersteund alsmede de evaluatie van deze processen (interne audits). Deze tool wil de gemeente Groningen voor langere periode aanschaffen om zo organisatie breed winst te kunnen behalen en te kunnen doorontwikkelen.

Het volgende kan worden vastgesteld over de gewenste situatie:

- De ICT-oplossing wordt gebruikt (o.b.v. eigen en domein specifieke normenkaders) om vast te stellen of en in hoeverre de werking van processen voldoet aan de gestelde wet- en regelgeving en waarmee opzet, bestaan en werking worden aangetoond;
- De ICT-oplossing maakt gebruik van de PDCA-cyclus (Plan, Do, Check, Act) om de kwaliteit (en werking) van de processen vast te kunnen stellen en te verbeteren;
- De ICT-oplossing bevat functionaliteit om controlerende taken uit te voeren of te verzenden naar proceseigenaren (bewijslast) om zodoende (periodiek) een beeld te vormen over de werking en kwaliteit van processen binnen de gemeente Groningen;
- De oplossing ondersteunt in het opstellen van het auditjaarplan en de uitvoering daarvan;
- De ICT-oplossing moet breed toepasbaar zijn op meerdere domeinen/ organisatieonderdelen binnen de gemeente Groningen;
- De ICT-oplossing beschikt over rapportagemogelijkheden waarmee eenduidig gerapporteerd kan worden over het bestaan en de kwaliteit van processen, maatregelen, risico's, naleving van wet- en regelgeving en verbeteringen;
- De inrichting en werking van de ICT-oplossing is de basis voor kwaliteitsmanagement voor organisatieonderdelen die op dit moment een latente behoefte hebben aan een ICT-oplossing.

4.2 PROCESBESCHRIJVING

Onderstaand de procesbeschrijving waarin het generieke werkproces voor de verschillende organisatieonderdelen staat geschetst.



5 AANTALLEN

De gemeente Groningen telt ca 5800 medewerkers, die overigens niet allemaal van het ICT-oplossing gebruik zullen maken. Gemeente Groningen voorziet dat (nu) de medewerkers van de afdelingen IB, Security, Auditing en Privacy de hoofdgebruikers zullen zijn van de beoogde ICT-oplossing. Zij zullen vanuit die rol medewerkers in de 1^e en 2^{de} lijn "benaderen" voor informatieverstrekking en of rapporteren aan de 3^e lijn.

Met de kennis van nu verwacht gemeente Groningen dat de navolgende aantallen gebruikers als hoofdgebruikers per afdeling worden ingezet:

5.1 INFORMATIEBEHEER

- Circa 25 Informatieadviseurs
- Circa 200 directiemedewerkers voor informatieverstrekking

5.2 SECURITY

- Circa 7 securitymedewerkers
- Circa 150 directiemedewerkers voor informatieverstrekking

5.3 AUDIT & CONTROL

- Circa 10 auditmedewerkers
- Circa 250 directiemedewerkers voor informatieverstrekking en ontvangst van informatie

5.4 PRIVACY

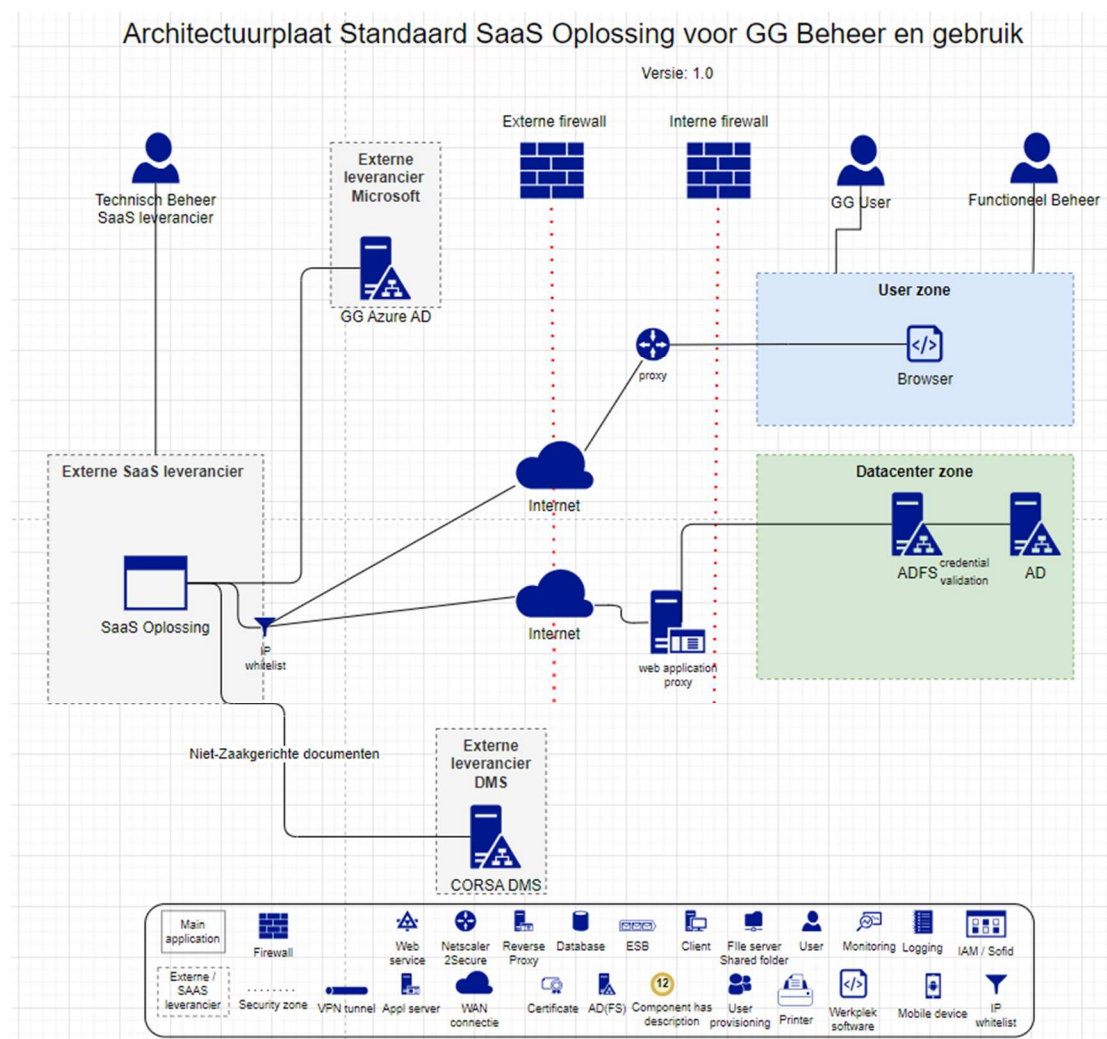
- Circa 5 privacy-medewerkers
- Circa 30 privacy-ambassadeurs van de 16 directies

6 ARCHITECTUUR

6.1 REFERENTIE-ARCHITECTUUR

De Gemeente Groningen hanteert een SaaS voor PaaS voor IaaS voor on-prem beleid. De te selecteren oplossing wordt een SaaS-oplossing, hiermee komen een aantal richtlijnen en standaarden mee. Zie daarvoor ook Bijlage 3 Programma van Eisen en Wensen.

De huidige situatie is een werkwijze die handmatig of door middel van Excel wordt uitgevoerd. Hier wordt in dit hoofdstuk geen aandacht aan besteedt, de gewenste situatie is geschetst in onderstaande afbeelding.



7 SCOPE VAN DE OPDRACHT

De scope van de opdracht, volgens de GIBIT2023 definitie de gevraagde 'ICT-prestatie', omvat in elk geval het volgende:

- Leveren van de Gebruikersrechten van de ICT-oplossing;
- Meehelpen met het opstellen van het definitieve Plan van Aanpak;
- Uitvoeren van het Implementatieplan, tenminste voor het bedrijfsonderdeel informatiebeheer met bijbehorend verandermanagement;
- Leveren van Opleidingen en overige Documentatie;
- In samenwerking met andere (derden) partijen voor (bv) het leggen van koppelingen;
- Leveren van 'Dienstverlening op Afstand' conform de Service Level Agreement en het Overeengekomen Gebruik (zie begrippenlijst GIBIT2023);
- Leveren van regulier Beheer op de Oplossing conform Beheermodel;
- Het kunnen leveren van Consultancy tijdens de beheerfase.

Na implementatie van de tooling en werkwijze voor Informatiebeheer kan in een vervolgtraject verder gewerkt worden aan het implementeren voor Security, Privacy en Audit & Control. Deze implementaties hebben een lagere prioriteit en vallen buiten scope van de opdracht.

Wij vragen u bij inschrijving **niet** om een 'exitplan' op te stellen.

8 CRITERIA

De selectie van de leverancier wordt gebaseerd op verschillende criteria, waarbij u moet denken aan bv de volgende onderdelen:

- Total Cost of Ownership van de oplossing over de gehele looptijd van het contract. Denk daarbij aan licenties, koppelingen, inrichting, implementatie, verandermanagement en exploitatie etc.
- Of de functionaliteit geschikt is voor de gehele organisatie;
- Mate waarin standaardisatie en best practices worden toegepast;
- Kwaliteit van de aangeboden Plan van Aanpak;
- Kwaliteit van het geboden beheer in uw Beheerplan;
- Gebruiksvriendelijkheid en trainingsmogelijkheden.

De uitwerking en weging van de diverse onderdelen zijn opgenomen in de "Offerteaanvraag GRC"

9 MARKTVERKENNING

In 2023 is een (vrijblijvende) marktverkenning voor een ICT-oplossing ten behoeve van het organisatieonderdeel Informatiebeheer uitgevoerd om te beoordelen of er standaardprogrammatuur (SaaS) in de markt aanwezig is die de behoefte van het organisatieonderdeel Informatiebeheer afdekt. Vijf marktpartijen hebben bij de gemeente Groningen een presentatie gegeven over hun visie over de toepassing van hun oplossing.

De marktverkenning heeft inzage gegeven in mogelijkheden die een ICT-oplossing biedt. Er is na de marktverkenning vastgesteld dat er een soortgelijke behoefte bestond bij meerdere organisatieonderdelen. Omdat bij het gemeente breed gebruiken van een ICT-oplossing bleek dat er een reële kans bestaat dat de geraamde opdrachtwaarde boven de aanbestedingsdrempel (€221.000,- exclusief BTW, gerekend over een periode van 4 jaar) uitkomt, is op basis van de marktverkenning besloten om een gemeente brede Europese Openbare aanbestedingsprocedure uit te voeren waarbij er breder gekeken wordt naar een geschikte generieke oplossing die bij meerdere organisatieonderdelen kan worden geïmplementeerd.

10 SAMENWERKING MET GEMEENTE GRONINGEN

10.1 IMPLEMENTATIE

Voor de implementatie zal Inschrijver nauw moeten samenwerken met gemeente Groningen. Daarom verzoekt gemeente Groningen om bij de inschrijving een concept PvA aan te leveren hoe inschrijver, met diens kennis en ervaring, de implementatie denkt uit te voeren. Na (voorlopige)gunning zal dit plan, in overleg met gemeente Groningen, als basis dienen voor een gezamenlijk PvA voor de wederzijdse samenwerking tussen Opdrachtgever en Leverancier om tot een succesvolle implementatie te komen.

Voor die implementatie stelt gemeente Groningen de nodige expertise beschikbaar om de implementatie goed te (bege)leiden.

Voor de projectfase/ implementatiefase voorziet gemeente Groningen op dit moment de inzet van de volgende rollen:

- Projectmanagement
- Architect
- Informatieadviseur
- Informatieanalist
- Functioneel beheer (test)
- Materiedeskundigen per deelgebied

10.2 EXPLOITATIE

Voor de Exploitatiefase verzoekt gemeente Groningen aan Inschrijvers om in een aan te leveren Beheerplan te beschrijven hoe het Beheer zal worden ingevuld door Inschrijver gezien diens expertise. In bijlage GRC Beheer model is omschreven hoe gemeente Groningen dit beheer voor zich ziet.

11 SAMENWERKING MET SOFTWARE INTEGRATOR

Het beheer van een groot deel van de ICT-omgeving van de gemeente Groningen wordt momenteel uitgevoerd door de software integrator Fujitsu Technology Solutions. Er zijn afhankelijkheden op het gebied van authenticatie en autorisaties en toegang tot applicaties. De technische afstemming van de implementatie van de ICT-oplossing zal dus in samenwerking en afstemming met Fujitsu plaatsvinden.

Het is niet uit te sluiten dat er met meerdere dienstverleners van de gemeente Groningen samengewerkt dient te worden. De gemeente Groningen verwacht van elke leverancier een proactieve houding.

12 TIJDLIJNEN

12.1 AANBESTEDINGSFASE

In de Offerteaanvraag is de planning van de Europees openbare aanbestedingsprocedure beschreven.

12.2 CONTRACT- EN VERIFICATIEFASE

Wij streven ernaar om tijdens de offerteverificatiefase, doch vóór definitieve gunning (ondertekening van de overeenkomst) de tijdlijnen voor de implementatiefase en de beheerfase in goed overleg vast te stellen. Daardoor zijn de resources van gemeente Groningen, de Leverancier en derde partijen op elkaar af te stemmen.

12.3 VOORBEREIDING IMPLEMENTATIE

Na definitieve gunning zal het definitieve Plan van Aanpak worden vastgesteld.

De ambitie is om binnen 2 maanden na ondertekening van de overeenkomst te starten met de implementatie.

12.4 IMPLEMENTATIEFASE

Het voornemen is om na een succesvolle implementatie GRC, en PRD dus live staat, met IB projectmatig te starten met een tweetal PDCA-cycli met 2 Directies (BurgerZaken en (vermoedelijk) StadsOntwikkeling.

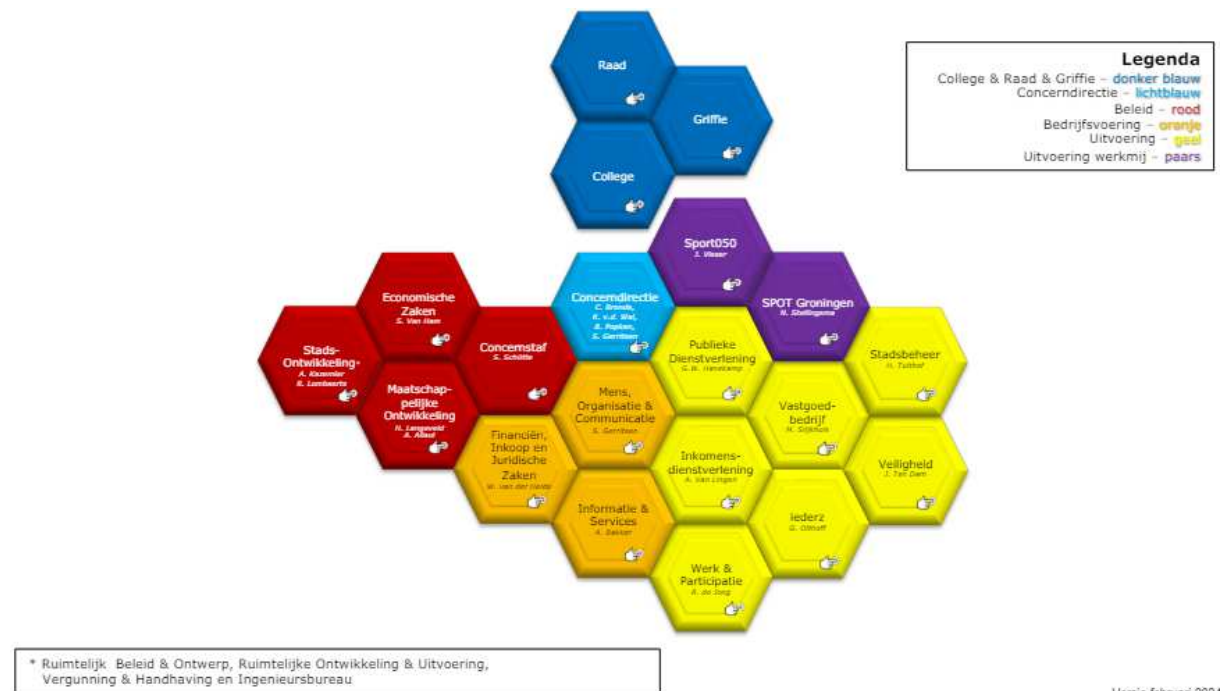
De overige disciplines zijn voor de implementatie buiten project scope geplaatst. Of dit zo blijft, is een nog te nemen Stuurgroep besluit.

12.5 BEHEERFASE

De looptijd van de overeenkomst start vanaf de Go-livedatum met een initiële periode van vijf jaar. Vervolgens kan de gemeente Groningen driemaal verlengen met een periode van twee jaar.

13 ORGANOGRAM GEMEENTE GRONINGEN

Ter informatie



College: het college van burgemeester en wethouders zoals bedoeld in artikel 5 van de Gemeentewet.

Gemeentesecretaris: de secretaris zoals bedoeld in artikel 100 de Gemeentewet. De gemeentesecretaris is ook de algemeen directeur en daarmee de hoogste leidinggevende van de ambtelijke organisatie.

Concerndirectie: de gemeentesecretaris en de concerndirecteuren vormen samen de concerndirectie.

Concerndirecteur: de leidinggevende die de gemeentesecretaris bijstaat in de uitvoering van diens taken, die verantwoordelijk is voor de resultaten van het toegewezen domein (en de daartoe behorende directies) en de toegewezen concernopdrachten/-opgaven of (begrotings)programma's. Daar waar de gemeentesecretaris hiërarchisch verantwoordelijk is voor een onderdeel, wordt de gemeentesecretaris eveneens begrepen onder de aanduiding concerndirecteur.

Directie: de organisatie-eenheid die onder de hiërarchische leiding staat van een of meerdere directeuren. De directie bestaat uit samenhangende afdelingen, teams, projecten en/of programma's.

Directeur: de leidinggevende die met het management van een directie is belast en die verantwoording aflegt aan één van de concerndirecteuren of aan de gemeentesecretaris.

Programma: samenhangende verzameling van (veelal) maatschappelijke doelen en prestaties (bestaande uit deelprogramma's, beleidsvelden en activiteiten) met daarvoor vastgestelde middelen.

Project: samenhangende activiteiten die worden uitgevoerd om op een planmatige manier een bepaald doel te bereiken binnen een afgesproken tijd. Een project is tijdelijk en eenmalig en richt zich op een concreet resultaat.

Concerncontroller: de functionaris belast met de toetsing van de informatie(voorziening), het zorgdragen voor controlsystemen en de onafhankelijke advisering van het college en de concerndirectie over sturing en beheersing van de organisatie.

Functionaris Gegevensbescherming (FG): de functionaris die als interne toezichthouder bij de gemeente Groningen toe ziet op de naleving van de wet- en regelgeving rond de bescherming

van persoonsgegevens. De Algemene verordening gegevensbescherming (AVG) en de Wet politiegegevens (Wpg) zijn de wettelijke basis voor het toezicht van de FG.

Hoofdstructuur organisatie

Binnen de gemeente onderscheiden we drie domeinen. Onder elk domein vallen directies die aan specifieke onderwerpen en taken werken.

- Sociaal Maatschappelijk domein, met directies:
 - Maatschappelijke Ontwikkeling (DMO)
 - Inkomensdienstverlening
 - Werk & Participatie
 - Iederz
 - SPOT
 - Sport050
- Ruimtelijk Economisch domein, met directies:
 - Stadsontwikkeling - Ruimtelijk Beleid en Ontwerp
 - Stadsontwikkeling - Ruimtelijke Ontwikkeling en Uitvoering
 - Vastgoedbedrijf
 - Economische Zaken
- Domein Dienstverlening, met directies:
 - Stadsbeheer
 - Publieke Dienstverlening
 - Shared Service Center - Informatie & Services
 - Shared Service Center - Mens, Organisatie en Communicatie
 - Shared Service Center - Financiën, Inkoop en Juridische Zaken
 - Shared Service Center - Facilitair, Services en Huisvesting
- Naast deze genoemde directies zijn er nog twee andere directies:
 - Veiligheid
 - Concernstaf