AANBESTEDING GRC

BIJLAGE 13 DEMONSTRATIE CASUSSEN

1 INHOUDSOPGAVE

2 INLEIDING

Dit document beschrijft de te demonstreren casussen voor Informatiebeheer, Privacy, Security en Audit en Control. De casussen dienen uitvoerbaar te zijn in de GRC met auditfunctionaliteit-oplossingen (vanaf hier: de ICT-oplossing) van de Inschrijvers.

Middels de beschreven casussen krijgt Gemeente Groningen een completer beeld over de mogelijkheden, onmogelijkheden, (bredere) toepasbaarheid en van de gebruiksvriendelijkheid van de mogelijke ICT-Oplossing(en) vanuit verschillende Inschrijvers.

3 INFORMATIEBEHEER

3.1 ALGEMEEN

Eén van de organisatieonderdelen die gebruik gaat maken van de ICT-oplossing is Informatiebeheer. Informatiebeheer is verantwoordelijk voor het bewaren, beheren, archiveren/ vernietigen en toegankelijk houden van overheidsinformatie. Als één van de primaire gebruikers van de ICT-Oplossing is er een casus uitgewerkt waarin een goed beeld kan worden verkregen van de mogelijkheden en gebruiksvriendelijkheid waarmee de ICT-Oplossing ingezet kan worden.

3.2 CASUS: GC8A INFORMATIEBEHEER

We onderkennen de volgende actoren voor deze casus:

Kwaliteitsmedewerker Informatiebeheer	Bewaakt de kwaliteit van de processen en uitvoering op basis van de gestelde wet- en regelgeving.
Informatiebeheerder	Voert kwaliteitscontroles uit op basis van de gestelde normen vanuit de wet- en regelgeving.
Proceseigenaar	Is eigenaar/ verantwoordelijke voor de processen die uitgevoerd worden.

3.2.1 UITVOERING CASUS: INFORMATIEBEHEER

1. De **Kwaliteitsmedewerker Informatiebeheer** kan in de ICT-Oplossing een taak uitzetten naar de **Informatiebeheerder** om een steekproef te houden naar de kwaliteit van de digitale dossiers over een bepaalde periode van een werkproces;
2. De **Informatiebeheerder** accepteert deze taak in de applicatie, voert de kwaliteitscontroles uit en legt de resultaten vast in de applicatie;
3. De ICT-Oplossing genereert een rapportage waaruit blijkt of gecontroleerde dossiers voldoen aan de gestelde kwaliteitsnormen en of dat er verbetermaatregelen moeten worden getroffen;
4. De rapportage wordt in de applicatie als taak aangeboden aan de **Proceseigenaar** van het werkproces waartoe de gecontroleerde dossiers behoren.;
5. De **Proceseigenaar** accepteert de gedane resultaten en mogelijke verbeteracties door de rapportage in de applicatie te valideren.

3.2.2 UITKOMSTEN VAN DE CASUS: INFORMATIEBEHEER

Onderdeel	Toelichting	Vastgelegde attributen
Taak aangeboden	▪ Er is een taak aangeboden ▪ Er is vastgelegd in de logging dat de taak is aangeboden door de kwaliteitsmedewerker Informatiebeheer aan de Informatiebeheerder	Type taak, status, tijdstip, aangemaakt door, toegewezen aan
Taak geaccepteerd	▪ Er is een taak geaccepteerd door Informatiebeheerder ▪ Er is vastgelegd in de logging dat de taak is geaccepteerd door Informatiebeheerder	Type taak, status, tijdstip, aangemaakt door, toegewezen aan
Uitvoering kwaliteitscontroles	▪ Er zijn kwaliteitsnormen toegepast en gecontroleerd ▪ Er is vastgelegd wat de uitkomsten zijn van de controles ▪ Er is vastgelegd welke bevindingen en/ of beheersmaatregelen er zijn.	Toegepaste kwaliteitsnormen, bevindingen, verbetermaatregelen, goedkeuring
Rapportage	▪ Er wordt een overzicht gegeven van de gecontroleerde kwaliteitsnormen, bevindingen en beheersmaatregelen ▪ Er wordt een rapportage verzonden (via de ICT-Oplossing) naar de proceseigenaar	Toegepaste kwaliteitsnormen, geregistreerde bevindingen, beheersmaatregelen, goedkeuring of afwijzing

4 AUDITING

4.1 ALGEMEEN

Auditing evalueert op strategisch, tactisch, operationeel, financieel niveau de organisatie op processen van governance, risk en compliance die relevant zijn voor de continuïteit van de bedrijfsactiviteiten en het realiseren van de doelen van gemeente Groningen. Op basis van een risicoanalyse wordt een auditjaarplan vastgesteld waaruit blijkt welke processen (en met welke frequentie) er gecontroleerd wordt.

4.2 CASUS: GC8B AUDITING

We onderkennen de volgende actoren voor deze casus:

Teamleider Auditing	Stelt op basis van een audit(riks) univers en een risicoanalyse het auditjaarplan op, bewaakt de voortgang van de auditplanning en kwaliteit van uitvoering van de audits. Monitort de opvolging van bevindingen.
Auditor	Voert onafhankelijk financiële-, operationele- en IT-audits en adviesopdrachten uit op basis van uitgevoerde risicoanalyses. Hierbij wordt de uitvoering en samenspel 1e en 2de lijn beoordeelt.
Auditleider	Geeft leiding aan het auditteam dat een opdracht uitvoert.
Proceseigenaar	Is eigenaar en integraal verantwoordelijk voor de interne beheersing en het realiseren van de doelen voor het object van onderzoek.

4.2.1 UITVOERING SCENARIO: AUDITING

a) De **teamleider Auditing** kan in de ICT-Oplossing een audit (risk)univers aanmaken waarin alle mogelijke auditobjecten zijn opgenomen.
b) De **teamleider Auditing** kan voor alle objecten in de audit univers een risicoanalyse op basis van risico factoren uitvoeren. De uitkomst vormt de input voor het auditjaarplan.
c) De **Auditleider** kan in de ICT-Oplossing een (audit)dossier aanmaken voor de controle van Opzet, Bestaan en Werking van een auditobject;
d) De **Auditorleider/auditor** stelt een procesrisicoanalyse voor het desbetreffende audit object
e) De **Auditorleider/auditor** selecteert uit een lijst beheersmaatregelen die benodigd zijn voor de 'scope' van deze audit.
f) De **Auditorleider/auditor** verkrijgt inzicht in de resultaten uit eerdere toetsingen van beheersmaatregelen door 1ste, 2de en 3de lijn ter voorbereiding op de uitvoering van de audit.
g) De **Auditorleider/auditor** stelt een werkprogramma op in de ICT-Oplossing welke invulling geeft aan de ICT-Oplossingcontrole van Opzet, Bestaan en Werking van een auditobject.
h) De **Auditor** voert het werkprogramma uit en legt de resultaten vast in de ICT-Oplossing en op documentatie.
i) De **Auditleider** voert een review uit op de uitgevoerde werkzaamheden en legt de reviewpunten terug bij de **Auditor** ter opvolging
j) De ICT-Oplossing genereert een overzicht waaruit blijkt of de beheersmaatregelen in opzet, bestaan en werking effectief zijn.
k) De **Auditleider** stelt een rapportage op in de ICT-Oplossing op basis van beschikbare informatie.
l) De **teamleider auditing** voer een review uit op de auditrapportage, waarna de **Auditleider** reviewpunten opvolgt.
m) De **auditleider** selecteert de bevindingen waarvan de opvolging wordt gemonitord en zet deze uit bij de **proceseigenaar**.

4.2.2 UITKOMSTEN VAN DE CASUS: AUDIT & CONTROL

Onderdeel	Toelichting	Vastgelegde attributen
Auditjaarplan opstellen (1&2)	▪ Er is een audit univers inclusief risicoanalyse opgesteld als input voor het auditjaarplan door de teamleider Auditing	Auditobjecten, risico classificatie, Audit univers, status, tijdstip, aangemaakt door, gewijzigd door, goedgekeurd door,
Dossier aanmaken	▪ Er is een dossier aangemaakt door de Auditleider	Dossier
Inrichten audit (4 t/m 7)	▪ Er is een plan uitgewerkt hoe de audit wordt vormgegeven en uitgevoerd ▪ Er is vastgelegd in de logging wie welke taak heeft uitgevoerd en wie wat heeft gereviewd.	Proces stappen, proces risico's, beheersmaatregelen, werkstappen, status, tijdstip, aangemaakt door, voor de werkstappen: toegewezen aan
Taak geaccepteerd	▪ De Auditor heeft taken uit het werkprogramma toegewezen gekregen	Type taak, status, tijdstip, aangemaakt door, toegewezen aan
Uitvoering Audit	▪ De werkstappen uit het werkprogramma zijn uitgevoerd ▪ Er is vastgelegd wat de uitkomsten zijn van de testwerkzaamheden. ▪ Er is vastgelegd welke bevindingen (positief en negatief) er zijn. ▪ Er is bewijslast vastgelegd dat Opzet, Bestaan en Werking bevestigd van het werkproces. ▪ Er zijn relaties gelegd tussen de uitkomsten van de testwerkzaamheden en de bewijslast. ▪ Het systeem logt wie de uitvoering van de taken op zich heeft genomen	Toegepaste kwaliteitsnormen, bevindingen, goedkeuring, bewijslast (documenten), status, tijdstip, aangemaakt door,
Review audit	▪ De uitgevoerde testwerkzaamheden worden door de auditleider 'gereviewd' en waar nodig voorzien van review opmerkringen ▪ De review wordt gelogd binnen de ICT-Oplossing	Status, (review)opmerkingen, tijdstip, aangemaakt door, toegewezen aan
Review opvolging	▪ De auditor volgt de review punten die van de auditleider zijn ontvangen op en biedt de stukken opnieuw ter review aan. ▪ De opvolging wordt gelogd binnen de ICT-Oplossing	Opvolging review, status, tijdstip, aangemaakt door, toegewezen aan
Rapportage	▪ Er wordt een overzicht gegeven van de gecontroleerde **beheersmaatregelen** en uitkomsten ▪ De auditleider stelt op basis van het inzicht een rapportage met toelichting vanuit de ICT-Oplossing ▪ De Teamleider audit voert een review uit op de rapportage en legt review punten terug aan de auditleider ▪ De Auditleider volgt reviewpunten op. ▪ De uitgevoerde werkstappen worden gelogd.	Toegepaste kwaliteitsnormen, geregistreerde bevindingen, beheersmaatregelen, rapportage, status, tijdstip, aangemaakt door, toegewezen aan

5 PRIVACY

5.1 ALGEMEEN

Sinds de komst van de Algemene verordening gegevensbescherming (AVG) heeft Privacy het verwerkingsregister op orde gemaakt. Binnen dit register wordt bijgehouden waar, hoe en in welke processen persoonsgegevens worden verwerkt. Om de governance te bewaken is er een behoefte aan een oplossing waarmee er kan worden toegezien op de uitvoering van het beleid en in hoeverre deze toereikend is of dat er beheersmaatregelen moeten worden toegepast.

5.2 CASUS: GC8C PRIVACY

We onderkennen de volgende actoren voor deze casus:

Privacy officer/ ambassadeur	Bewaakt de governance over de processen die raakvlak hebben met de AVG-wetgeving en initieert de Data protection impact assessment(s) (DPIA) bij de proceseigenaren en ziet er op toe dat deze bij wijzigingen (of na verlopen van geldigheid) wordt herzien.
Proceseigenaar	Voorziet de Privacy Officer van de Data protection impact assessment(s) (DPIA) en volgt eventuele adviezen op bij bevindingen.

5.2.1 UITVOERING SCENARIO: PRIVACY

a) De **Privacy Officer** vraagt een Data protection impact assessment (DPIA) op bij de **Proces eigenaar**
b) De **Proces eigenaar** ontvangt een taak met de betreffende uitvraag van de DPIA
c) De **Proces eigenaar** specificeert de taak en bevestigt
d) De **Privacy Officer** ontvangt een notificatie van de afgeronde taak en beoordeelt het vastgestelde risico in de DPIA

5.2.2 GEGEVENS DIE UITGEVRAAGD WORDEN IN DEZE CASUS

We vragen de volgende gegevens uit (zie ook Bijlage 14 PIA format gemeente Groningen)

- 1x Impact verhogende aspecten
  - Te classificeren naar: Laag, Middel, Hoog
- 1x Kans verhogende aspecten
  - Te classificeren naar: Laag, Middel, Hoog
- 1x Maatregelen ter verlaging van impact
  - Te classificeren naar: Must have, Should have, Could have
- 1x Maatregelen ter verlaging van kans
  - Te classificeren naar: Must have, Should have, Could have

5.2.3 TOELICHTING OP PROCES

De onderstaande procesomschrijving geeft weer hoe de DPIA op dit moment worden toegepast en hoe het risico wordt vastgesteld.

Invul instructie

Voordat er een risico inschatting gedaan kan worden met betrekking tot de gegevensverwerking is het van belang basis informatie over de gegevensverwerking te verzamelen. Deze informatie vul je in op het tabblas **Basisinfo**. Vervolgesn ga je naar het tabblad **Invulsheet** voor de risico inschatting.

Risico = Kans * Impact

In het kader van deze PIA wordt er op een aantal onderdelen naar het risico gekeken:
1. Type project
2. Aard van de gegevens
3. Betrokken partijen
4. Verzamelen
5. Gebruik
6. Bewaren en vernietigen
7. Beveiligen

Om tot een goede risico inschatting te komen zijn in de bijgevoegde matrix per onderdeel een aantal impact en kans verhogende apecten benoemd. De spreadsheet biedt ruimte om per aspect een inschattig te maken (Laag, Middel, Hoog). Uiteindelijk gaat het erom deze te vertalen naar een inschatting van de Impact en de kans op onderdeel niveau. Als je op onderdeel niveau de waardes voor impact en kans invult dan wordt het risico automatisch berekend.

Impact verhogende aspecten	Impact			Kans verhogende aspecten	Kans			Risico
	L	M	H		L	M	H	
Type project	L					M		Laag
Omvang				Onvoldoende duidelijkheid over verantwoordelijkheid over data				
Publieke belangstelling				Onvoldoende onderbouwing van data behoefte				
				Gebruik van nieuwe technologieën				
				Betrokkenheid meerdere (ook externe)partijen				
Aard van de gegevens								Onbekend
Gebruik bijzondere persoonsgegevens				Hoeveelheid personen waarover data verzameld wordt.				
Hoeveelheid identificerende gegevens				Aantal personen/instanties dat toegang heeft tot de informatie				
Gegevens kunnen basis zijn voor beoordeling van gedrag of prestatie van het individu				Onvoldoende beveiliging van de data				

De volgende risico matrix is daarvoor gebruikt.

	Kans Laag	Kans Middel	Kans Hoog
Impact Laag	Risico Zeer Laag	Risico laag	Risico Middel
Impact Middel	Risico Laag	Risico Middel	Risico hoog
Impact Hoog	Risico Middel	Risico Hoog	Risico Zeer Hoog

Het beperken van risico's richt zich op het verkleinen van de impact en/of het verkleinen van de kans. Bijbehorende maatregelen zijn per onderdeel in de spreadsheet weergegeven. Op basis van de risico inschatting kan aangegeven worden hoe groot de noodzaak is voor het treffen van de maatregel:

- M - Must : maatregel wordt vereist
- S - Should: maatregel wordt dringend gewenst
- C - Could: maatregel is gewenst maar niet noodzakelijk

Figuur 1 Uitvraag DPIA

5.2.4 UITKOMSTEN VAN DE CASUS: PRIVACY

Onderdeel	Toelichting	Vastgelegde attributen
Taken	▪ Taken kunnen worden toegewezen aan een Proces Eigenaar door de Privacy Officer	Taak, Toegewezen door, Toegewezen aan, Einddatum
Data protection impact assessment (DPIA)	▪ Er worden zowel aspecten vastgelegd en geclassificeerd alsmede de maatregelen.	Impact verhogende aspecten, Kans verhogende aspecten, Maatregelen ter verlaging van impact, Maatregelen ter verlaging van kans, Classificaties
Classificatie aspecten	▪ Per aspect dat wordt beoordeeld kan er een classificatie worden meegegeven die van toepassing is op het uitgevraagde aspect. Elk aspect kan worden beoordeeld middels een classificatie: Laag, Middel, Hoog. Het totaaloverzicht stelt vast in hoeverre er sprake is van impactvolle of kans verhogende aspecten waarvoor adviezen afgegeven kunnen worden.	Aspecten, classificatie (Laag, Middel, Hoog)
Classificatie Maatregelen	▪ Per maatregel kan worden vastgesteld of deze moet, zal of kan toegepast worden.	Maatregelen, classificatie (Must have, Should have, Could have)

6 SECURITY

6.1 ALGEMEEN

Gemeenten verantwoorden zich over informatiebeveiliging en kwaliteit middels de ENSIA. ENSIA staat voor: Eenduidige Normatiek Single Information Audit. De ENSIA beidt een gestructureerde verantwoording voor informatiebeveiliging die (door middel van de BIO) door de Nederlandse overheid wordt gesteld aan Nederlandse Gemeenten.

Figuur 2 Bron: VNG/ ENSIA

6.2 CASUS: GC8D SECURITY

Vanuit Security (Informatiebeveiliging) wordt er jaarlijks een aanlevering gedaan aan de ENSIA waarmee de verantwoording aan de Gemeenteraad (en aan de toezichthouder van het Rijk) in één keer kan worden gedaan.

We onderkennen de volgende actoren voor deze casus:

Security officer	Bewaakt de governance over de processen die raakvlak hebben met de eisen die gesteld worden aan informatiebeveiliging en is coördinator voor de verantwoording aan ENSIA (Vereniging van Nederlandse Gemeenten).

6.2.1 UITVOERING SCENARIO: SECURITY

1. De **Security Officer** haalt via de oplossing de antwoorden (op vragenlijsten) van het vorige auditjaar op uit ENSIA
2. De **Security Officer** stelt vast in hoeverre de gegevens nog actueel zijn voor het nieuwe jaar waarover verantwoording vastgelegd moet worden
   De **Security Officer** levert de bijgewerkte gegevens opnieuw aan richting ENSIA

6.2.2 UITKOMSTEN VAN DE CASUS: SECURITY

Onderdeel	Toelichting	Vastgelegde attributen
Vragen lijst (voorgaand jaar)	▪ Het is mogelijk om de gegevens uit voorgaande jaren te gebruiken als basis voor het nieuwe jaar.	Opgehaalde vragen en antwoorden (voorgaand jaar)
Vragen lijst (toekomstig jaar)	▪ Het is mogelijk om de gegevens aan te leveren aan ENSIA en daarmee de verantwoording aan zowel de Gemeentelijke als toezichthouders van het Rijk te voldoen.	Vragen en antwoorden (nieuwe jaar)