EngageProcess

Case Study

Holistische aanpak van **GRC** binnen de Gemeente Maastricht



Gemeente Maastricht

Over deze Case..

Governance, Risk & Compliance (GRC) draait om het realiseren van organisatiedoelen op een verantwoorde en efficiënte manier, met oog voor risico's en onzekerheden. Tegelijkertijd is het belangrijk om wendbaar te blijven in een steeds veranderende omgeving. De uitdaging is dan ook: hoe behoud je flexibiliteit zonder de controle over processen te verliezen? Hoe zorg je ervoor dat medewerkers zich bewust zijn van de risico's? En hoe genereer je rapportages die altijd actueel zijn? Voor effectief GRC-beheer is het essentieel om procesmanagement als fundament te zien en hierop verder te bouwen.

Bij de Gemeente Maastricht is gekozen voor een integrale, procesgerichte benadering, ondersteund door het Engage Process platform. Hiermee worden processen inzichtelijk gemaakt en worden risico's en beheersmaatregelen gekoppeld aan specifieke processtappen. Medewerkers kunnen binnen hun eigen werkcontext relevante risico's bespreken en bijbehorende documentatie raadplegen. Dit vergroot de betrokkenheid en draagt bij aan een organisatie brede bewustwording rondom risico's en compliance.

In deze case study worden verschillende begrippen gebruikt. Hieronder geven we van elk van die begrippen een korte omschrijving.

CFW: Control Framework

AVG: Algemene Verordening Gegevensbescherming

PDCA-cyclus: De PDCA-cyclus (Plan, Do, Check, Act) is een methode om processen continu te verbeteren. Je plant een actie, voert die uit, controleert het resultaat en past waar nodig aan.

Deming-cirkel: De Deming-cirkel is een kwaliteitsmodel voor continue verbetering, opgebouwd uit de stappen PDCA. Ondersteunt bij het systematisch werken.

GEMMA: Gemeentelijke Modelarchitectuur is een standaard van de VNG (Vereniging van Nederlandse Gemeenten) om informatiesystemen en processen van gemeenten op elkaar af te stemmen.

Sterrenmodel: Een procesvolwassenheidsmodel dat door Engage Process gebruikt wordt.

COSO Framework: Een internationaal model voor risicobeheer en interne controle binnen organisaties.

SoX-richtlijnen: SoX-richtlijnen (Sarbanes-Oxley Act) zijn regels om de betrouwbaarheid van financiële verslaglegging te vergroten en fraude te voorkomen.

VIC-controle: VIC (Verbijzonderde Interne Controle) is een vorm van interne controle die zich richt op het toetsen van o.a. rechtmatigheid, getrouwheid en effectiviteit.

AO/IC-principes: Administratieve Organisatie (AO): de manier waarop processen, procedures en verantwoordelijkheden binnen een organisatie zijn ingericht. Interne Controle (IC): de maatregelen die worden genomen om te controleren of processen goed verlopen en risico's worden beheerst.

RISMAN-methodiek: Een gestructureerde aanpak voor risicomanagement: risico's identificeren, beheersmaatregelen formuleren, risico's monitoren en evalueren.

Visie en strategische verankering



De Gemeente Maastricht heeft een duidelijke ambitie uitgesproken: in 2030 moet procesmanagement de ruggengraat van de organisatie zijn. Deze visie vormt de basis voor de manier waarop Governance, Risk & Compliance (GRC) wordt benaderd. Door processen centraal te stellen, ontstaat een directe verbinding tussen strategie, uitvoering en verantwoording. De missie, visie en strategie van de gemeente vormen het kader voor het ontwerp en de inrichting van alle processen. Deze zijn vastgelegd in het Control Framework (CFW), dat volledig is uitgewerkt in Engage Process.

Uitgangspunten en werkwijze

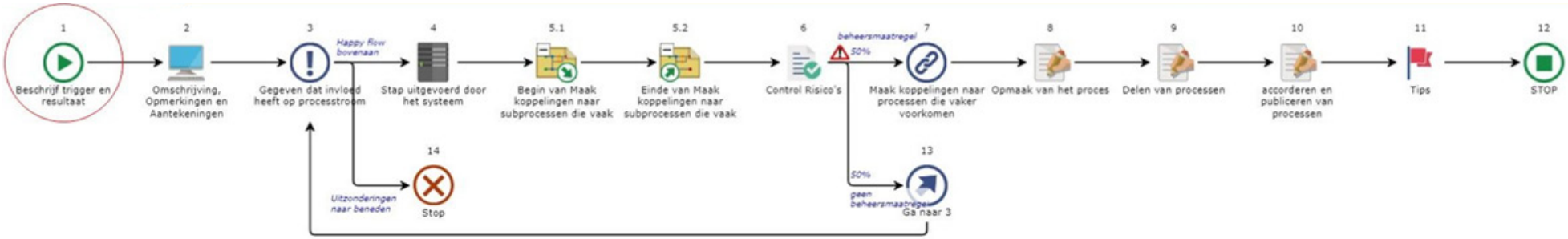
Procesmanagement helpt de Gemeente Maastricht om strategische doelen te vertalen naar de dagelijkse praktijk en grip te houden op de operationele processen waarmee dagelijks waarde wordt geleverd. Om dit te ondersteunen zijn zes doelstellingen geformuleerd: optimalisatie van de bedrijfsvoering, transparantie en controle via proceskaarten, centralisatie van procesadvies duidelijk eigenaarschap per proces, een integrale benadering van processen (inclusief o.a. AVG, control en KPI's), en samenwerking als gedeelde verantwoordelijkheid binnen de hele organisatie.

Binnen deze aanpak wordt onderscheid gemaakt tussen het feitelijke proces en het procesmodel zoals afgesproken. De proceskaarten vormen de basis voor sturing en verantwoording. Daarbij wordt ook onderscheid gemaakt tussen procesbeheersing en procesbeheer. Procesbeheersing richt zich op het uitvoeren en verbeteren van processen via de PDCA-cyclus, met een centrale rol voor proceseigenaren en uitvoerende medewerkers. Procesbeheer faciliteert dit door systemen in te richten, informatie beschikbaar te stellen en ondersteuning te bieden, met betrokkenheid van o.a. procesondersteuners, controllers en adviseurs.

Deze rollen komen samen in het procesverbeterteam, dat werkt aan dagelijkse verbeteringen, structurele aanpassingen en grotere optimalisatieprojecten. Het team stimuleert continu verbeteren op basis van de Deming-cirkel, waarbij de proceseigenaar verantwoordelijk blijft voor de implementatie van verbeteringen.

Eenduidige manier van modelleren

De procesarchitectuur van de Gemeente Maastricht sluit aan op GEMMA en is herkenbaar gemaakt in Engage Process. Er is een gezamenlijke modelleermethodiek ontwikkeld, vastgelegd in een handleiding voor procesbeheerders en -eigenaren. Het sterrenmodel geeft aan hoe processen gemodelleerd moeten worden; belangrijke processen worden minimaal op 3-sterrenniveau vastgelegd, inclusief activiteiten, rollen, resultaten, risico's en beheersmaatregelen.

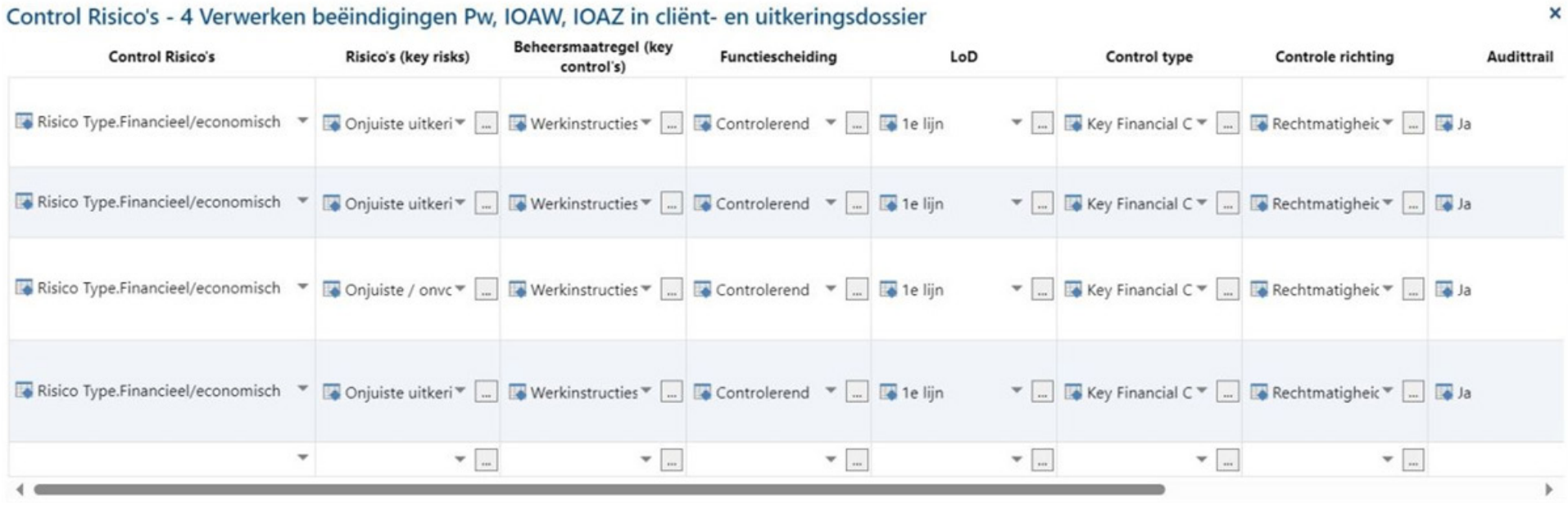


Deze uniforme werkwijze zorgt voor een gedeeld begrippenkader en vormt een control framework waarmee processen vergelijkbaar zijn, risico's geanalyseerd kunnen worden en verbeteringen centraal worden doorgevoerd. Voor kwaliteitsborging toetsen Adviseurs Procesmanagement de proceskaarten, terwijl Strategisch Adviseurs Informatievoorziening zorgen voor aansluiting op strategie en beleid.

Gebruik van tabellen voor Risico's en beheersmaatregelen

In Engage Process kunnen vooraf tabellen worden ingericht om risico's en beheersmaatregelen direct te koppelen aan processen en/of processtappen. De Gemeente Maastricht heeft samen met de afdeling Control een tabel ontwikkeld op basis van het COSO-control framework en SoX-richtlijnen. Dit model ondersteunt bij het verbeteren van interne beheersing en risicomanagement. Op de volgende pagina's worden verschillende ingerichte tabellen toegelicht. Onderstaande schermafdruk dient slechts ter illustratie.

Op de volgende pagina's worden verschillende ingerichte tabellen toegelicht. Onderstaande schermafdruk dient slechts ter illustratie.



① Risico's (Key Risks)

Deze kolom beschrijft de risico's die voortkomen uit het werkproces. Er is geen vaste lijst; risico's zijn proces- en situatiespecifiek. Vaak hebben de risico's wel te maken met een van de controledoelstellingen en/of controlecriteria bijvoorbeeld het risico dat een aanvraag niet juist en/of volledig is, risico dat zorg niet doelmatig wordt geleverd, risico dat prestatie niet wordt geleverd etc.

② Beheersmaatregelen (Key Controls)

Beheersmaatregelen worden afgestemd op het specifieke risico en op maat beschreven. Binnen het COSO-control framework en de daaruit afgeleide SoX-omgevingen worden de beheersmaatregelen onderverdeeld in **de volgende categorieën:**



Generieke beheersmaatregelen: 4-ogenprincipe, management reviews, autorisatieprocedures, aansluitcontroles, monitoring- en uitzonderingsrapportages, beleidsdocumenten, werkinstructies, fysieke toegangsbeveiliging, verbijzondere controles (2e lijns VIC-controles) en interne audits (3e lijn).



IT-controls: toegangsbeveiliging, back-up & recovery, changemanagement (w.o. gebruikerstest en acceptatieprocedures) en incidentmanagement (w.o. registratie en periodieke analyse).



Organisatorische beheersmaatregelen: governance-organisatiestructuur, directieteam besluit, heldere functieprofielen, training en opleiding, resourcemanagement (w.o. werving en selectie), communicatieprocedures en verzekeringen.

③ Functiescheiding

Op basis van AO/IC-principes (Starreveld) worden functies onderscheiden: beschikken, bewaren, controleren, registreren en uitvoeren.

④ Line of Defense

De kolom Line of Defense geeft aan in welke verdedigingslinie een control valt: de eerste lijn voert uit, de tweede lijn ondersteunt en monitort, en de derde lijn toetst onafhankelijk op effectiviteit.

⑤ Control Type / Doelstelling

Er wordt onderscheid gemaakt tussen twee typen controls: een Key Control richt zich op het borgen van doeltreffendheid en doelmatigheid, terwijl een Key Financial Control de getrouwheid en rechtmatigheid waarborgt. Het control type is gekoppeld aan de doelstelling:



Getrouwheid (KFC)



Rechtmatigheid (KFC)



Doeltreffendheid (KC)



Doelmatigheid (KC)

⑥ Control Criterium

In deze kolom worden de **9 control criteria** genoemd zoals die in de kadernota rechtmatigheid zijn opgenomen en zijn daarmee per definitie een key financial control:



Calculatiecriterium



Valuteringscriterium



Adresseringscriterium



Volledigheidscriterium



Aanvaardbaarheidscriterium



Leveringscriterium



Begrotingscriterium



Voorwaardencriterium



Misbruik en Oneigenlijk gebruik criterium

7 Risicotype

Deze kolom onderscheidt verschillende typen risico's voor risicomanagement en rapportagedoeleinden. Op basis van de RISMAN-methodiek worden risico's geclassificeerd vanuit zeven invalshoeken: politiek/bestuurlijk, financieel/economisch, juridisch/wettelijk, technisch, organisatorisch, geografisch/ruimtelijk en maatschappelijk.
Daarnaast zijn ook de risicotypen fraude en imago opgenomen.

8 Audit Trail

In deze kolom wordt met 'Ja' of 'Nee' vastgelegd of de control op een objectieve wijze aan de hand van onderliggend bewijsmateriaal kan worden vastgesteld.

9 Specifieke beheersmaatregelen

In dit veld komt de specifieke toelichting op de control te staan.

Gebruik van rapportages

Rapportages vanuit Engage Process bieden inzicht en ondersteuning voor proceseigenaren en control. Ze helpen bij het beheren van eigenaarschap, doorlooptijden, rollen, applicaties en wijzigingsdata. Dit is essentieel voor het prioriteren binnen de PDCA-cyclus. Door in kolom 9 van de tabel de specifieke beheersmaatregelen te benoemen is het mogelijk om hiervan ook rapportages te genereren waarbij in één oogopslag duidelijk is welke specifieke beheersmaatregel(en) een bepaald risico in het werkproces afdekt. Hieronder een voorbeeld van zo'n GRC rapportage van de Gemeente Maastricht.

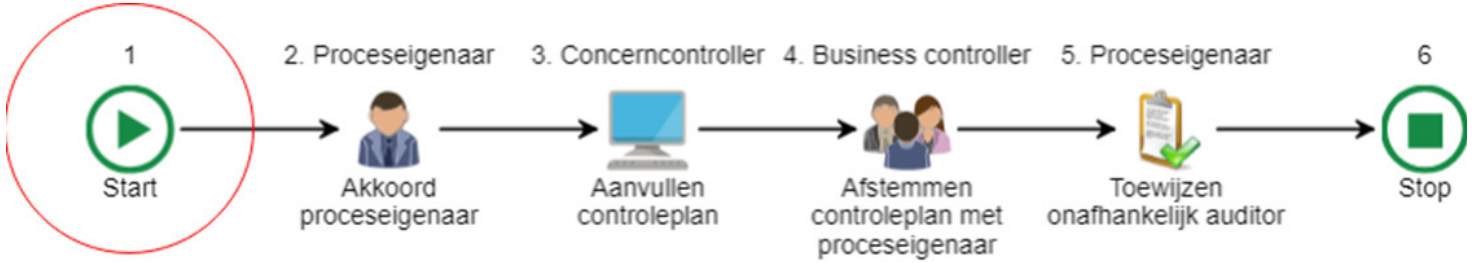
Rapportage GRC

Lijst

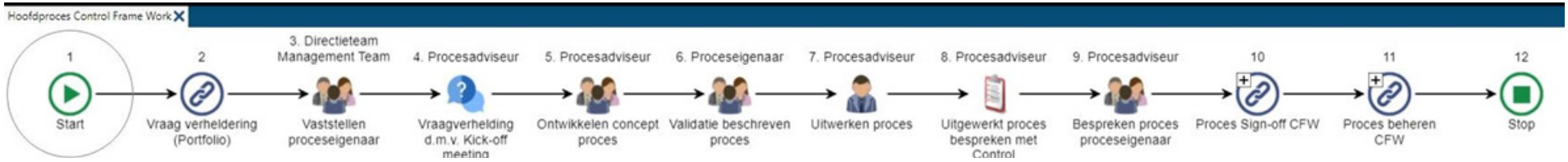
Proces	Processtap	Control Risico's	Risico's (key risks)	Beheersmaatregel (key control's)	Functiescheiding	LoD	Control type	Controle richting	Audittrail	Beheersmaatregel (specifiek)
Bestaande raamovereenkomst	5. Controleren financiele uitnutting raamovereenkomst	Risico Type.Financieel/economisch	Afdeling Juridische Zaken.niet voldoen aan regel en-wetgeving	Generiek.Interne audits 3e lijn	Functiescheiding.Controlerend	LoD.3e lijn	Control type.Key Financial Control (getrouwheid en rechtmatigheid)	Controle richting.Rechtmatigheid (key financial control)	Audittrail.Ja	Controle uitnutting/ raming van de raamovereenkomst. Risico : Uitnutting van de raamovereenkomst is reeds overschreden en dit is in strijd met de wet. Op het moment dat de applicatie "verplichtingenadministratie" is aangeschaft en up & running is, wordt de uitnutting automatisch bijgehouden. Interne audits: Controle facturen raamovereenkomst. Op dit moment nog geen rol toebedeeld aan interne auditors, zodra deze ingeregeld zijn dan volgt er een 2e lijns LoD.

Sign-off in Engage Process

Het goedkeuringsproces in Engage Process dient als sluitstuk van de PDCA-cyclus en waarborgt de actualiteit van de control frameworks. De proceseigenaar bevestigt hiermee de juistheid en volledigheid van processen, en dat risico's in beeld zijn en passende maatregelen zijn getroffen.



Hoofdproces control framework



Conclusie

De Gemeente Maastricht heeft een uniforme werkwijze voor procesmodellering en risicobeheersing ingericht in Engage Process. Door het gebruik van tabellen en duidelijke afspraken over modelleren, worden risico's en beheersmaatregelen direct gekoppeld aan processen en waar nodig aan processtappen. Dit vergroot de betrokkenheid van medewerkers en versterkt de grip op uitvoering en verantwoording. Het procesverbeterteam borgt continu verbeteren via een gestructureerde cyclus, met actieve inbreng van zowel proceseigenaren als uitvoerende medewerkers.

Het goedkeuringsproces in Engage Process vormt het sluitstuk van de PDCA-cyclus. Proceseigenaren bevestigen hiermee de actualiteit, juistheid en volledigheid van processen, en dat risico's in beeld zijn en beheersmaatregelen effectief zijn ingericht. Rapportages bieden daarbij waardevolle ondersteuning voor eigenaarschap, doorlooptijden, rollen en wijzigingen, en maken het mogelijk om beheersmaatregelen gericht te monitoren.



EngageProcess

EngageProcess

Over Engage Process

Engage Process biedt een eenvoudige en zeer effectieve manier voor het in kaart brengen en analyseren van je bedrijfsprocessen. Het platform is 100% SaaS en stelt je team in staat om processen samen te bespreken, te evalueren en te verbeteren.
Door de medewerker op de eerste plaats te zetten, is Engage Process een echte human-centric oplossing. Dit betekent proactief processen verkennen en opnieuw vormgeven in real-time.

Processen vormen de basis voor managementprogramma's zoals compliance, rechtmatigheid, risicomanagement, continu verbeteren en digitale transformatie . Meer dan 300 organisaties in Nederland en wereldwijd zetten Engage Process dagelijks in, waaronder Gemeente Ede, Flanderijn, Provincie Noord-Holland, Woonmeij, Centrada, City of Edinburgh Council, H2O groep, CIZ en SCS Railways.

HOOFDKANTOOR

Tel: **+31 20 530 72 80**
Email: sales@engageprocess.com
Website: engageprocess.com
Kantoor: **Boeingavenue 8**
1119 PB, Schiphol-Rijk

UK OFFICE

Phone: **+31 20 530 72 80**
Email: sales@engageprocess.com
Website: engageprocess.co.uk
Office: 3 Waterhouse Sq, Greater
London, England EC1N 2SW