

Architectuur en koppelingen

GRC Tool

GRC Tool
20230925 Architectuur en koppelingen
Datum september 2023
Joop Jansen

Inhoudsopgave

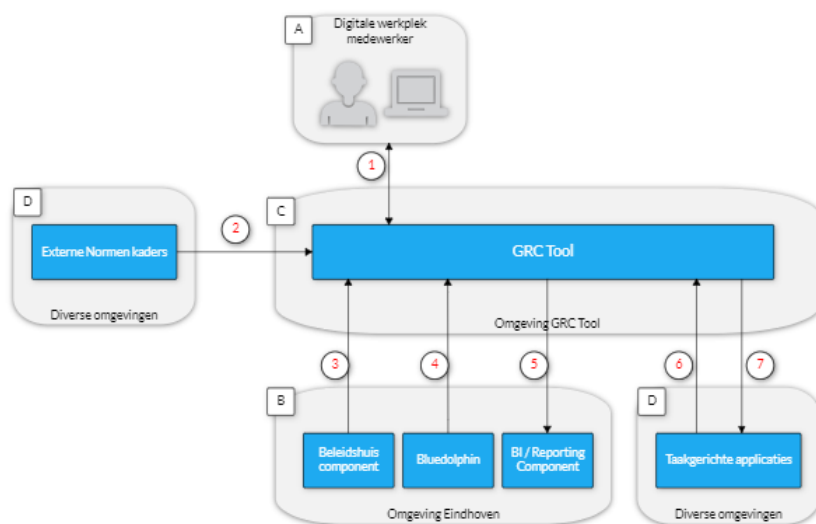
Inleiding.....	3
1 Omgevingen	3
(A): Omgeving digitale werkplek gemeente Eindhoven.....	3
(B): Omgeving gemeente Eindhoven.....	3
(C): Omgeving GRC Tool	4
(D): Diverse Omgevingen.....	4
2 Koppelingen.....	4
1 Medewerker vanuit digitale werkplek gemeente Eindhoven	4
2 Externe Normenkaders	5
3 Data uitwisseling vanuit de Beleidshuiscomponent.....	5
4 Data uitwisseling met Bluedolphin.....	5
5 GRC naar BI / Reporting component	5
6 Taakgerichte applicaties naar GRC	5
7 GRC naar Taakgerichte applicaties	5

Inleiding

De GRC Tool ondersteunt gemeente Eindhoven breed het “in control” traject. Dit omvat zowel Finance als Managerial & Operational control en IT related controls, door het managen van Governance, Risico management en Compliance (GRC) binnen de organisatie.

Naast een centrale inrichting kunnen de sectoren (Concern) Control, I&B, CIO waaronder Privacy en Security hun beheer, risico, mitigatie eisen en audit processen daarop zelf inrichten.

Onderstaande afbeelding (Figuur1) is de grafische weergave van de relevante applicatieomgevingen van de GRC Tool en de daarbij behorende koppelingen. Bij iedere omgeving is een letter geplaatst en bij iedere koppeling een nummer, deze worden in hoofdstuk één en twee beschreven.



Figuur 1: Context GRC Tool

1 Omgevingen

(A): Omgeving digitale werkplek gemeente Eindhoven

Dit is de omgeving waarin de medewerker van de gemeente Eindhoven werkt. Het kan elke medewerker in elke rol zijn. De Medewerker krijgt toegang tot het GRC via een standaard webbrowser. Uiteraard hoort hier een identificatie-, authenticatie- en autorisatiemechanisme bij dat voldoende beveiliging en betrouwbaarheid biedt.

(B): Omgeving gemeente Eindhoven

De GRC Tool draait in de omgeving van de aanbieder als een zogenaamde Cloud applicatie en wisselt gegevens uit met informatiesystemen binnen de omgeving van de gemeente Eindhoven. Hiervoor zijn de volgende integratie- en beveiligingscomponenten in gebruik:

Firewall & Reverse Proxy/Load Balancer

Voor alle koppelingen geldt dat gegevensuitwisseling veilig gebeurt conform de informatiebeveiligingseisen. Een secure verbinding vanuit de SaaS aanbieder is op basis van SSL en een officieel PKI-certificaat, conform de richtlijnen van het Nationaal Cyber Security Center (TLS1.2 of hoger). Er wordt geen directe koppeling naar interne systemen vanaf het internet toegestaan deze loopt altijd via de Firewall->Reverse Proxy/Load Balancer->Enterprise Service Bus->Doel Systeem.

Integratieplatform

Geautomatiseerde gegevensuitwisseling tussen een SaaS applicatie en interne IV-systemen van de gemeente Eindhoven verloopt via het Integratieplatform van de gemeente Eindhoven. Eén van de componenten de ESB OpenTunnel wordt op dit moment vervangen door WSO2.

Alle nieuwe koppelingen die via de ESB lopen worden met WSO2 gerealiseerd. Dit zal altijd op basis van geldende en actuele standaarden zijn. Daarnaast wordt API Management binnen het Integratieplatform gerealiseerd.

Geautomatiseerde gegevensuitwisseling tussen verschillende SaaS applicaties van de gemeente Eindhoven verloopt altijd via het integratieplatform van de gemeente.

(C): Omgeving GRC Tool

Vanuit een Cloud omgeving biedt de GRC Tool de medewerkers toegang tot de applicatie. Er vindt hierbij gegevensuitwisseling plaats met diverse andere systemen in verschillende omgevingen. De autorisatie en authenticatie wordt uitgevoerd door GRC en GRC garandeert de vertrouwelijkheid van de informatie in het systeem door ervoor te zorgen dat alleen de personen voor wie de informatie bedoeld is er toegang toe hebben op basis van een toegekende gebruikersrol.

(D): Diverse Omgevingen

De GRC Tool ondersteunt gemeente breed het “in control” traject. Dit omvat alle bedrijfsprocessen die ondersteund worden door taakgerichte applicaties. Deze taakgerichte applicaties staan in diverse (cloud) omgevingen.

2 Koppelingen

In dit hoofdstuk worden de koppelingen (data uitwisselingen) beschreven, volgens de nummering die is aangegeven in figuur 1.

Voor de GRC tool wordt verwacht dat alle genoemde data uitwisselingen kunnen worden gerealiseerd.

Koppelingen tussen systemen zijn noodzakelijk op het moment dat er gegevens van een bronsysteem gebruikt moeten worden in een ander systeem, het doelsysteem. De gewenste gegevens uit het bronsysteem moeten beschikbaar worden gemaakt en vervolgens op een veilige manier getransporteerd worden naar het doelsysteem waarin de gegevens geïntegreerd worden opgenomen.

Per koppeling geldt het volgende:

Om het transport van de data van bronsysteem naar doelsysteem mogelijk te maken kan uit verschillende patronen gekozen worden:

1. Out of the Box koppeling. Dit is veelal een koppeling volgens een generieke standaard met landelijke partijen zoals CBS, Belastingdienst, KvK en banken of bijvoorbeeld een koppeling met de Azure AD van de gemeente.
2. Realtime berichtenverkeer (via webservices / api) altijd via Integratieplatform
3. Berichten verkeer (via webservices / api) altijd via Integratieplatform
4. Geautomatiseerde bestandsoverdracht
5. Andere geautomatiseerde oplossing
6. Handmatig Download / Upload

De patronen staan in volgorde van voorkeur, waarbij patroon 1 de meeste voorkeur heeft en patroon 6 de minste voorkeur. Iedere koppeling kent echter een specifieke situatie en dus per koppeling zal naar het hoogst mogelijke, werkbare patroon worden gestreefd. Voor de ene koppeling is dit bijvoorbeeld patroon 1, maar bij een andere koppeling is dit niveau 4. In dit hoofdstuk staan de benodigde koppelingen beschreven met vermelding van het minimaal geëiste patroon.

Belangrijk is dat de data uitwisseling altijd aan de vereisten van informatiebeveiliging voldoet.

Boven de genoemde 6 integratiepatronen wil de gemeente in de toekomst gebruik maken van streaming integration. Dit biedt een flexibele en robuuste manier om datastromen door een informatielandschap heen te organiseren. Daarmee is het in te zetten als een moderne, cloud-native vorm van ETL ten behoeve van data integratie met het dataplatform.

Van de reeds bestaande koppelingen is hieronder de huidige situatie beschreven met aandachtspunten voor de nieuwe situatie.

1 Medewerker vanuit digitale werkplek gemeente Eindhoven

Doel	Medewerker krijgt na het inloggen op de gemeentelijk Active Directory op basis van SSO geautoriseerde toegang tot GRC
Patroon	Minimaal patroon 1 - Out of box koppeling t.b.v. authenticatie (Single Sign On / Multi Factor Authenticatie)
Toe te passen Standaard	OAuth / SAML 2.0 protocol

2 Externe Normenkaders

Doel	Hierbij worden externe normenkaders geleverd aan de GRC Tool
Patroon	Minimaal patroon 6 - Handmatig Download / Upload
Toe te passen Standaard	
Technische realisatie	

3 Data uitwisseling vanuit de Beleidshuiscomponent

Doel	Hierbij wordt data vanuit de beleidshuiscomponent geleverd aan de GRC Tool. Denk hierbij aan: kaders en richtlijnen en procedures & controle punten
Patroon	Minimaal patroon 6 - Handmatig Download / Upload
Toe te passen Standaard	
Technische realisatie	

4 Data uitwisseling met Bluedolphin

Doel	Hierbij wordt procesbeschrijvingen geleverd aan de GRC Tool
Patroon	Minimaal patroon 6 - Handmatig Download / Upload
Toe te passen Standaard	
Technische realisatie	

5 GRC naar BI / Reporting component

Doel	GRC voedt de BI / Reporting component
Patroon	Minimaal patroon 6: Handmatige download / upload
Toe te passen Standaard	
Technische realisatie	Toepassen richtlijnen vanuit het Dataplatform

6 Taakgerichte applicaties naar GRC

Doel	Hierbij wordt data vanuit de Taakgerichte applicaties geleverd aan de GRC Tool. Denk hierbij aan: Inge vulde vragenlijsten en bewijzen en onderkende risico's
Patroon	Minimaal patroon 6: Handmatige download / upload
Toe te passen Standaard	
Technische realisatie	

7 GRC naar Taakgerichte applicaties

Doel	Hierbij wordt data vanuit de GRC Tool geleverd aan de Taakgerichte applicaties. Denk hierbij aan: toegewezen rollen, Governance assessment(vragenlijsten), bevindingen / verbeterpunten, mitigerende maatregelen
Patroon	Minimaal patroon 6: Handmatige download / upload
Toe te passen Standaard	
Technische realisatie	