

Programma van Eisen

Cloud basis Platform

Organisatie: BIJ12

Versie: v2.0

Datum: Augustus 2025

Status: Definitief

Inleiding	3
Achtergrond	3
Doel van dit document	3
Business Drivers	3
Scope en Uitgangspunten	3
Projectdoelstellingen en Randvoorwaarden	4
Doelstellingen:	4
Randvoorwaarden:	4
Eisen	4
Functionele Eisen	4
Niet-functionele Eisen	5
Integraties en Compatibiliteit	5
Kwaliteitseisen	6
Beheer- en Ondersteuningseisen	6
Planning en Mijlpalen	7
Globale projectplanning	7
Belangrijke mijlpalen	8
Afhankelijkheden	8
Acceptatiecriteria	8
Documentatie Vereisten	10
Technische documentatie	10
Gebruikers documentatie	10
Governance documentatie	10
Bijlagen	10

Inleiding

Achtergrond

BIJ12 ondersteunt provincies en het Rijk bij ruimtelijke opgaven en beheert gezamenlijke uitvoeringsorganisaties. Om deze missie effectief te kunnen blijven vervullen in een digitaliserende samenleving, is modernisering van de IT-infrastructuur essentieel.

De huidige Azure omgeving is organisch gegroeid en mist een gestructureerde governance en security baseline. Dit leidt tot:

- Inconsistente security policies
- Beperkte schaalbaarheid voor nieuwe initiatieven
- Verhoogde operationele complexiteit - Suboptimale cost management

Doel van dit document

Dit Programma van Eisen (PvE) definieert de functionele en niet-functionele eisen voor:

- Het Azure High Level Design van een nieuwe cloud basis platform
- De implementatie van Azure Landing Zones volgens het Microsoft Cloud Adoption Framework Enterprise Scale model
- De governance, security en operationele structuur voor toekomstige workload adoptie

Business Drivers

- Digitale transformatie: Ondersteuning van moderne, cloud-native oplossingen
- Security & Compliance: Voldoen aan overheidsstandaarden en regelgeving
- Operational Excellence: Gestandaardiseerde, geautomatiseerde processen
- Cost Optimization: Transparante en gecontroleerde cloud uitgaven
- Schaalbaarheid: Flexibele infrastructuur voor toekomstige groei

Scope en Uitgangspunten

Binnen scope:

- Implementatie van nieuwe Azure Landing Zone architectuur (Cloud Basis Platform) volgens Cloud Adoption Framework
- Migration van governance naar CAF Enterprise Scale model
- Security baseline en identity management setup
- Operationele procedures en monitoring

Buiten scope:

- Migratie van bestaande workloads (separaat project)
- On-premises infrastructuur wijzigingen
- Applicatie-specifieke aanpassingen

Projectdoelstellingen en Randvoorwaarden

Doelstellingen:

- Inrichten van CAF-gebaseerde landing zones volgens het Enterprise-Scale model.
- Bieden van een solide basis voor governance, security, networking en compliance.
- Implementatie van best practices volgens CAF.
- Realiseren van een werkende en bruikbare landing zone-omgeving waarin nieuwe workloads direct kunnen landen en beheerd worden.
- Ondersteuning van huidige en toekomstige workloadmigraties vanuit on-prem of andere cloudomgevingen.

Randvoorwaarden:

- Gebruik van Azure Policy, Management Groups en Blueprints.
- Aansluiting op Azure tenants en IAM-setup. Seperaat traject IAM-implementatie.
- Ondersteuning voor hybride scenario's (Azure Arc, ExpressRoute, VPN).

Eisen

Functionele Eisen

- Azure Landing zone implementatie volgens de Microsoft best practices.
- Alle Azure resources moeten logs verzenden naar centrale Log Analytics workspace met minimaal 90 dagen retentie (Azure Monitor, Defender).
- Basisrollen (RBAC) en toegang via PIM voor platformbeheer moeten zijn ingericht.
- Automatische provisioning van resources via pipelines (IaC met Bicep of Terraform).

Niet-functionele Eisen

- Minimale beschikbaarheid van 99,9% op platformcomponenten.
- 24/7 support van cloud leverancier
- Performance optimalisatie m.b.v. onder andere: Azure Front Door, Azure DNS en caching waar relevant.
- Governance-tracking via Azure Policy, Cost Management en Tagging-strategieën.
- Schaalbaarheid als basisgedachte meetbaar via IaC, gebruik van cloud-native solutions, alle administratieve taken geautomatiseerd.
- Bij alle keuzes voor geolocaties altijd binnen EU, liefst binnen NL.
- AVG proof en BIO-Coompliant. Inclusief logging & audit-trail.

Integraties en Compatibiliteit

1. Identity & Toegang

Integratie met het SSO/IAM model. Daarmee dus integratie met Azure Entra ID.

- SSO en ondersteuning voor Microsoft Entra multifactor authenticatie (MFA)
- Authorisatie via RBAC-model.
- Ondersteuning voor Conditional Access policies.

2. Landingzones – Hub-Spoke model

- Het voorbereiden van landen van de applicatieworkloads (informatieproducten) via HUB-SPOKE model en de bijbehorende netwerkvraagstukken om deze goed af te schermen.

3. Toekomstige integraties & compatibiliteit

- De oplossing moet voorbereid zijn op aansluiting met bestaande en toekomstige workloads binnen het BIJ12 landschap.
- De oplossing moet ondersteuning bieden voor API's en event driven communicatie.
- Het gebruik van Microsoft-componenten danwel open source componenten die in de markt standaard zijn en een hoge compatibiliteit hebben, hebben sterk de voorkeur.

Kwaliteitseisen

- Alignment met CAF Enterprise-scale referentiearchitectuur.
- Alle technische documentatie (inclusief ontwerpbesluiten, netwerkinrichting, RBAC en deployed resources etc.) moet up-to-date zijn en revisietijden bevatten.
- Periodieke Cloud Adoption Framework, Well-Architected Review en Security Baseline assessment. En bij oplevering minstens 1 keer uitgevoerd volgens deze richtlijnen.
- Audit trail beschikbaar voor alle beheeracties via Azure Activity Log.

Beheer- en Ondersteuningseisen

Operationele beheer

- Processen definiëren en toetsen zodat de beheerpartij (nader te bepalen) deze kan overnemen
- Tot aan oplevering is de implementatiepartij degene die het operationeel beheer uitvoert.
- De basis van operationeel beheer zou markt richtlijnen dienen te volgen zoals ITIL.
- Het opvolgen van updates en andere security aangelegenheden zoals beveiliging preventief verhogen en het volgen bij de standaarden van de Cloud markt is een onderdeel hiervan.

Supportmodel

- Tot aan oplevering is de implementatiepartij degene die support op de landing zones uitvoert.
- Processen definiëren en toetsen zodat de beheerpartij (nader te bepalen) deze kan overnemen
- De basis van support zou markt richtlijnen dienen te volgen zoals ITIL.
- Afstemmen en integreren met het interne supportmodel is een onderdeel hiervan.

Monitoring en incidentbeheer

- Gebruik van Azure Monitor, Log Analytics en Application Insights voor real-time monitoring.
- Notificaties worden gedaan via Action Groups (e-mail, teams, sms-integratie)

- Logging en alerting worden centraal beheerd via een management subscriptie.

Wijzigingen & releasebeheer

- Wijzigingen worden gedaan in de Infrastructure-as-Code (IaC) en worden geautomatiseerd in Azure DevOps Pipelines.
- Wijzigingen worden voorzien van, Impactanalyse, backout-plan en goedkeuring indien nodig.
- Productiereleases gebeuren volgens een releasekalender, buiten piektijden en met monitoring

Lifecyclemanagement

Resources worden periodiek geëvalueerd op:

- Relevantie
- Kosten
- Beveiliging

Verouderde of ongebruikte resources worden gearhiveerd of verwijderd na goedkeuring.

Gebruik van **tags** is verplicht. Tags dienen de best practices te volgen van het CAF.

Planning en Mijlpalen

Planning en mijlpalen volgens implementatie criteria van het CAF. Echter BIJ12 heeft wat specifieke planning en mijlpalen bedacht, deze staan qua details in het PSA.

Globale projectplanning

Fase	Periode	Doelstelling
Initiatie & analyse	2025Q3	Vastleggen PvE, requirements, security-randvoorwaarden
Architectuur & HLD	2025Q3~Q4	Ontwikkelen HLD, netwerkinrichting, landing zones ontwerp
MVP realisatie	2025Q4	Bouw en configuratie van dataplatform met minimale scope
Test & acceptatie	2025Q4	Functionele validatie, performance test, security scan
Oplevering MVP	2025Q4	In productie nemen eerste versie met dashboards en ETL
Uitbreidingen & koppelingen	2025Q4~2026Q1	Integraties met externe bronnen (bijv. CBS, stikstofmodel)
Beheeroverdracht	2026Q1~Q2	Opleiding beheerders, overdracht documentatie

Eerste evaluatie & WAF	2026Q1	Well-Architected Review + kostenanalyse + optimalisatie
-----------------------------------	--------	---

Belangrijke mijlpalen

Mijlpaal	Deadline
PvE afgerond en goedgekeurd	aug 2025
Azure landing zone operationeel	sep/okt 2025
Eerste provincie-dashboard opgeleverd	nov/dec 2025
Volledige koppeling met externe datasets	dec 2025
Beheeroverdracht aan BIJ12 (start)	Feb/mrt 2026
Eerste evaluatie & optimalisatie ronde	2026 Q2

Afhankelijkheden

- Beschikbaarheid van BIJ12 IAM/SSO en Eviden/Atos inrichting tenants (Azure Entra ID integratie)
- Toegang tot externe databronnen (via API of bestandslevering)
- Beschikbaarheid van functionele product owners per applicatie
- Beschikbaarheid van beheerorganisatie voor overdracht

Acceptatiecriteria

Functionele acceptatie

De oplossing wordt als functioneel geaccepteerd wanneer aan de volgende voorwaarden is voldaan:

- Beheer en operationeel support documentatie is gereed.
- Beheer en operationeel support is overdraagbaar aan beheerpartij (nader te bepalen).
- De omgeving is klaar om workloads (informatieproducten) te laten landen via landingzones.
- Goedgekeurde gebruikers kunnen inloggen via Azure Entra ID en hun rechten worden correct toegepast.
- Compliance standaarden dienen opgevolgd te worden met minimale eisen:
 - Minimale BIO Compliancy level is 90%
 - Minimale ISO 27001/2013 level is 80%

- Minimaal Security level Cloud-Security inrichting is 80%
- Minimale CIS Benchmark v2.0.0 Security level is 80%

Technische acceptatie

De technische acceptatiecriteria omvatten:

- De infrastructuur is opgezet conform de CAF Enterprise-Scale architectuur en voldoet aan het goedgekeurde HLD.
- Alle componenten (networking, RBAC, monitoring, back-up) zijn ingericht en getest.
- Netwerkcommunicatie tussen hub en spokes werkt conform ontwerp, inclusief firewallregels en private endpoints.
- Alle IaC-componenten zijn opgeslagen in een gecontroleerde repository met versiebeheer.
- Beveiligingsinstellingen zijn aantoonbaar conform baseline (bijv. TLS 1.2+, geen public IP's, MFA actief).
- De omgeving voldoet aan de afgesproken SLA's en prestatie-eisen (o.a. responstijden, beschikbaarheid).

Operationele acceptatie

Voor operationele acceptatie gelden de volgende criteria:

- Beheerdocumentatie is volledig en beschikbaar (inclusief runbooks, toegangsmatrix, releaseproces).
- Monitoring, alerting en logging zijn volledig operationeel en getest.
- Operationeel beheerteam is getraind in het uitvoeren van basisbeheer en incidentafhandeling.
- De supportstructuur (L1–L3) is ingericht en contactpunten zijn bekend.
- Er is een fallback- of rollbackplan beschikbaar voor kritieke componenten.
- Beheeroverdracht is formeel vastgelegd met akkoord van zowel project- als beheerzijde.

Documentatie Vereisten

Technische documentatie

- High Level Design document (HLD)
- Low Level Design document (LLD)
- Project Eind Architectuur (PEA)
- Deployment guides
- Operational runbooks

Gebruikers documentatie

- End-user handleiding

Governance documentatie

- Policies en procedures
- Compliance rapportages
- Audit trails

Bijlagen

(nog geen)