

Handreiking

Gemeentelijke implementatierichtlijn Microsoft Azure

GGI-Cloud Expertisecentrum

Vereniging van Nederlandse Gemeenten

Nassaulaan 12

2514 JS Den Haag

Auteurs: Jan Brinkkemper, Geeske Logtmeijer, Pieter-Bas Nederkoorn

Datum: november 2025

Versie: 1.0

©Vereniging van Nederlandse Gemeenten, Den Haag, november 2025

Inhoudsopgave

Gemeentelijke implementatierichtlijn Microsoft Azure	4
Scope	4
Uitbested	4
Microsoft hulpmiddelen.....	5
Cloud Adoption Framework	5
Azure Landingzone Conceptual Architecture	5
Accelerators.....	6
Azure Verified Modules.....	6
BIO Initiative Policy Template	6
VNG hulpmiddelen	7
GT Microsoft Framework	7
Haven.....	7
Implementatieadvies.....	8
1. Voer integrale risicoafweging public cloud uit.....	8
2. Azure tenant aanvragen	8
3. Voer een data-risicoanalyse en DPIA uit	8
4. Implementeer Azure landingzones naar voorbeeld LCA en gebruik BIO Compliance Initiative Template	9
5. Richt governance in.....	9
6. Richt Cost Management in	9

Gemeentelijke implementatierichtlijn Microsoft Azure

Veel gemeenten maken gebruik van het Azure cloudplatform van Microsoft. Daarbij is het belangrijk om te voldoen aan wet- en regelgeving en informatiebeveiliging en privacy bescherming op een adequaat niveau in te richten. Daarvoor heeft het GGI-Cloud Expertisecentrum (GCE) deze implementatierichtlijn opgesteld.

De Informatiebeveiligingsdienst (IBD) heeft deze stukken gelezen en ziet geen risico's voor gemeenten om deze stukken te gebruiken. Wel wordt er benadrukt dat deze documenten ontwikkeld zijn vanuit een generieke context en dat de gemeente zelf de toepasbaarheid in de eigen situatie dient te bepalen. Vanwege de aard van de risico's is het van belang dat hoger management en bestuur deze afwegingen expliciet onderschrijven.

De implementatierichtlijn bestaat naast dit document uit de volgende bijlagen :

- [Integrale Risicoafweging Public-Cloud](#)
- [GT Microsoft Framework](#)
- [BIO Initiative Policy Template](#)
- [Microsoft Cloud Adoption Framework voor Azure](#)

Scope

Dit document is gericht op de verantwoorde inrichting van het platform als fundament en beschrijft de technische hulpmiddelen die voor het creëren van de Azure omgeving kunnen worden gebruikt. Kern van dit document is het gebruik van het [BIO Initiative Policy Template](#). Daarnaast wordt gerefereerd naar een aantal standaarden en richtlijnen die door Microsoft zijn benoemd in het [Microsoft Cloud Adoption Framework voor Azure](#) (CAF). Het document gaat niet in op het inrichten en migreren van workloads.

Uitbesteed

Dit document is met name relevant voor gemeenten die zelf hun Azure omgeving inrichten. Indien uw gemeente deze inrichting wil uitbesteden, dan kunt u de volgende eis opnemen in uw programma van eisen (PvE):

“De Azure tenant is afgenomen onder de voorwaarden van het GT Microsoft Framework. Bij het inrichten wordt het BIO Initiative Policy Template toegepast op de hele tenant.”

Zorg dat je als gemeente zelf periodiek de compliance van de inrichting controleert in het compliance dashboard, zie “Stap 5: Richt governance in”.

Microsoft hulpmiddelen

Cloud Adoption Framework

Microsoft biedt verschillende hulpmiddelen voor organisaties om te migreren naar de Azure public cloud. Deze zijn beschreven in het Cloud Adoption Framework (CAF). De context van het CAF is zeer breed. Het CAF behandelt strategische, beleidsmatige en organisatorische aspecten alsook best-practices voor de technische inrichting. Het CAF is voor gemeenten beschikbaar via de e-learning omgeving van MS: [Aan de slag met het Cloud Adoption Framework](#).

Azure Landingzone Conceptual Architecture

Onderdeel van het CAF is de [Azure Landingzone Conceptual Architecture](#) (LCA). Deze architectuur beschrijft een voorbeeld hiërarchie voor het inrichten van een Azure Landingzone en beschrijft de samenhang tussen 8 ontwerpgebieden:

Ontwerpgebied	Doelstelling
Beveiliging	Implementeer besturingselementen en processen om uw cloudomgevingen te beveiligen.
Beheer	Voor stabiele, doorlopende bewerkingen in de cloud dient beheer te zijn ingericht conform de baseline in het CAF voor zichtbaarheid, naleving van bewerkingen en het beveiligen en herstellen van resources.
Governance	Automatiseer het controleren en afdwingen van beleid.
Platformautomatisering en DevOps	In lijn brengen van de beste tools en sjablonen om uw landingzones en ondersteunende resources te implementeren.
Azure-facturering en Active Directory-tenant	De juiste instellingen voor het maken van tenants, subscriptions en facturering zijn belangrijke stappen.
Identiteits- en toegangsbeheer	Identiteits- en toegangsbeheer is een primaire grensbeveiliging in de public cloud. Het is de basis voor een veilige architectuur die voldoet aan alle normen.
Netwerktopologie en -connectiviteit	Beslissingen ten aanzien van netwerk en connectiviteit zijn een zeer belangrijk basisaspect van elke cloudarchitectuur.
Resourceorganisatie	Als de cloudimplementatie wordt opgeschaald hebben overwegingen voor abonnementsontwerp en de hiërarchie van beheergroepen invloed op governance, Operations Management en implementatiepatronen.

Wanneer de richtlijnen van de LCA worden gevolgd, dan zal de Azure Landingzone bestaan uit meerdere platform en application landingzones. Een platform landingzone biedt generieke functionaliteit voor toepassingen in de application landingzones. Hierbij kan gedacht worden aan identity of connectiviteit. Om een landingzone snel in te richten kunnen zogeheten Accelerators of Verified Modules gebruikt worden.

Accelerators

Een Accelerator is een script waarmee direct een landingzone geïmplementeerd kan worden volgens de richtlijnen en uitgangspunten van Microsoft (of eventueel van derden). Er zijn Accelerators voor zowel platform landingzones als voor application landingzones. Afhankelijk van de eisen dienen de juiste Accelerators gebruikt te worden. Ga je de Azure landingzone bijvoorbeeld beheren via de Azure Portal, dan kun je de Azure Platform Landing Zones Portal Accelerator gebruiken. Voor een landingzone met een specifieke toepassing (bijvoorbeeld draaien van VM's, API management etc.) kun je gebruik maken van [Accelerators](#) die specifiek voor deze toepassing een (application) landingzone implementeren. Accelerators herken je aan de button "Deploy tot Azure" (figuur 1).



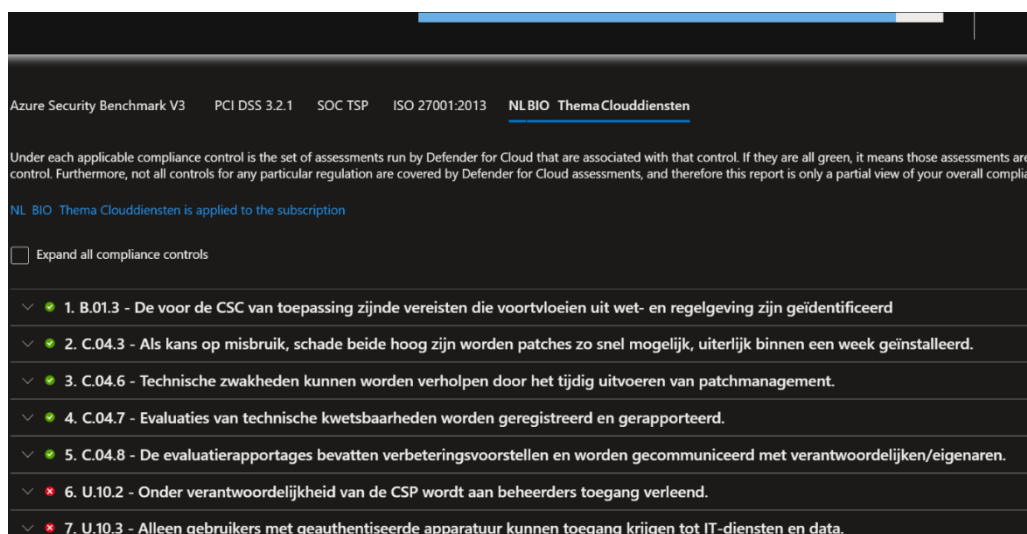
Figuur 1 Button activeren Accelerator

Azure Verified Modules

Er zijn ook Azure Verified Modules beschikbaar die gebruikt kunnen worden voor het implementeren van een landingzone. Een AVM is een script (Bicep of Terraform) waarmee een landingszone geïmplementeerd kan worden. Je gebruikt een AVM wanneer je de omgeving beheert middels Infrastructure as Code (IaC).

BIO Initiative Policy Template

Het [BIO Initiative Policy Template](#) bevat een set van policies die toegepast kan worden op een resource of meestal een set van resources binnen Azure. De policies zijn gemapt op de BIO controls waardoor inzichtelijk wordt in hoeverre de resources binnen Azure voldoen aan de (technische) BIO controls. In combinatie met Defender for Cloud kan via het Regulatory Compliance dashboard (figuur 2) inzichtelijk worden gemaakt in hoeverre de resources voldoen aan de BIO controls.



Figuur 2 Regulatory Compliance dashboard

VNG hulpmiddelen

GT Microsoft Framework

De VNG heeft in samenwerking met Microsoft een framework gerealiseerd waaronder alle gemeenten producten en diensten van Microsoft kunnen afnemen. Het framework bestaat uit juridische en commerciële voorwaarden voor Microsoft producten. Gemeenten kunnen een Azure tenant aanvragen onder voorwaarden van het GT Microsoft Framework.

Haven

Cloudagnostisch met behulp van containers

Het risico op leveranciers- en technology lock-in kunnen gemeenten beperken door de inzet van verschillende maatregelen. Gemeenten kunnen kiezen voor bepaalde technische inrichtingen en architectuurkeuzes, zoals containerisatie op een IaaS/PaaS-platform, die het makkelijker maken om workloads (applicaties, technische voorzieningen, dataverwerkingen e.d.) die men op een bepaalde Public Cloud dienst laat draaien, eventueel snel en eenvoudig naar andere omgevingen te verplaatsen. Bijvoorbeeld naar een on-prem omgeving of naar andere cloud omgevingen. De gemeentelijke [“Haven”-standaard](#) voor containerorkestratie helpt hierbij.

Implementatieadvies

In de vorige paragrafen zijn verschillende hulpmiddelen beschreven om een Azure tenant in te richten. Deze hulpmiddelen komen terug in het te volgen implementatieadvies. Het advies bestaat uit de volgende stappen die vervolgens verder worden toegelicht:

1. Voer een integrale risicoafweging public cloud uit
2. Vraag de Azure tenant aan
3. Voer een data-risicoanalyse en DPIA uit
4. Implementeer Azure landingzones naar voorbeeld LCA
5. Richt governance in
6. Richt Cost Management in

1. Voer integrale risicoafweging public cloud uit

Voordat een gemeente een Microsoft Azure omgeving in gebruik neemt, is er door de betreffende IT-afdeling, het hogere management en bestuurders een aantal afwegingen te maken. Afwegingen ten aanzien van de beoogde voordelen, mogelijke risico's en daarbij te treffen beheersmaatregelen. In de [Integrale Risicoafweging Public-Cloud](#) worden de belangrijkste aspecten beschreven die een rol spelen bij deze afweging.

2. Azure tenant aanvragen

Uitgangspunt is dat de producten zijn afgenomen onder de voorwaarden van het GT Microsoft Framework. Hiermee wordt juridisch een aantal essentiële onderdelen geregeld.

3. Voer een data-risicoanalyse en DPIA uit

Middels een risicoanalyse op de beoogde data en processen kan bepaald worden welk beveiligingsniveau toegepast moet worden op de tenant en daarbinnen in te richten landingzones. Gaat het bijvoorbeeld om een laagvertrouwelijke omgeving zoals een “sandbox” die alleen bedoeld is om zaken uit te proberen en waarbinnen uitsluitend fictieve data wordt gebruikt? Of is een reguliere of zelfs hoog vertrouwelijke omgeving gewenst? Om dit te bepalen is een risicoafweging noodzakelijk. Dit kan bijvoorbeeld met behulp van de [Baselinetoets BBN BIO](#).

Indien een hoog-vertrouwelijke omgeving nodig is, dan biedt Microsoft diverse opties. Je kunt kiezen om Azure op een lokale infrastructuur te gebruiken of voor een configuratie onder de naam “sovereign cloud”, inclusief bijvoorbeeld encryptie tijdens verwerking van data (confidential computing).

Binnen een tenant kunnen landingzones voorkomen met verschillende beveiligingsniveau's. Om hoge kosten te voorkomen is een nauwkeurige risicoafweging essentieel.

DPIA herijken

Wanneer een workload die in de public cloud wordt geplaatst gemeentelijke data bevat, dient de gemeente vooraf de DPIA's, behorende bij deze data en processen, te herijken voor de gewijzigde techniek en bijbehorende risico's. Gemeenten kunnen hiervoor de [generieke DPIA's](#) voor cloudproducten hergebruiken.

4. Implementeer Azure landingzones naar voorbeeld LCA en gebruik BIO Compliance Initiative Template

Implementeer de relevante landingzones op basis van functionele behoefte naar voorbeeld van het LCA. Maak daarbij gebruik van de juiste Accelerators dan wel AVM's. Let erop dat je bij het aanmaken van een landingzone kiest voor een regio binnen de EER.

Pas op het hoogste niveau (meestal de Tenant Root Group) het BIO Compliance Initiative Template toe. Daarmee wordt deze policyset automatisch toegepast op alle onderliggende resources/resourcegroups. Het policy-effect, de actie die wordt uitgevoerd wanneer wordt geconstateerd dat een bepaalde resource niet aan een policy voldoet, staat op 'Audit'. Dit zorgt ervoor dat melding wordt gedaan in de activity log wanneer een resource niet aan de (BIO) policies voldoet. Het aanmaken wordt niet gestopt. Audit zorgt voor minder continuïteitsrisico en zorgt ervoor dat in sommige gevallen bewust kan worden afgeweken. Hier kan bijvoorbeeld behoefte aan zijn bij gebruik van een sandbox-omgeving.

Om *bewust* af te wijken is het noodzakelijk dat voor elke resource die niet voldoet een exceptierapport is opgesteld. Hierin is o.a. vermeld waarom de resource niet voldoet, wat de mogelijke risico's zijn van het niet voldoen, eventuele acties die zijn uitgevoerd om deze risico's te mitigeren en een formele acceptatie van de restrisico's.

Middels het toevoegen van extra policies op lagere niveaus, kan voor specifieke resources (of groepen van resources bijvoorbeeld binnen een landingzone), een strengere regime geconfigureerd worden.

Op basis van de gewenste functionaliteit worden vervolgens de relevante application landingzones ingericht. Indien beschikbaar, kunnen hiervoor ook Accelerators of AVM's gebruikt worden.

Na het creëren van resources zal Microsoft de "pay per use" kosten in rekening gaan brengen.

Bij het aanmaken van de resources is het ook goed om rekening te houden met eenduidige naamgeving en het taggen van resources. Door hier vooraf over na te denken, bijvoorbeeld door middel van een namingconvention, kunnen later snel en eenvoudig (kosten)rapportages en overzichten aangemaakt worden.

5. Richt governance in

Het inrichten van de governance gaat over diverse aspecten zoals inrichten van beheerrollen, kennismanagement, leveranciersmanagement, costmanagement, etc.

Voor de controle op de technische inrichting is het in ieder geval van belang om het volgende frequent te controleren.

Wanneer policies in 'Audit'-mode staan, zullen deze telkens wanneer een overtreding wordt geconstateerd een melding maken in de security log. Deze logs moeten regelmatig gecontroleerd worden. Daarnaast kan via het Regulatory Compliance dashboard op elk moment bekeken worden in hoeverre wordt voldaan aan de (technische) BIO vereisten. Wij adviseren gemeenten om hun dashboard regelmatig te raadplegen en hierover te rapporteren binnen de eigen organisatie.

6. Richt Cost Management in

Azure public cloud omgevingen kunnen exponentieel groeien. Om te voorkomen dat je achteraf verrast wordt door hoge kosten of bijvoorbeeld betaalt voor ongebruikte resources of dubbele workloads is het belangrijk om de kosten te bewaken. Dat kan bijvoorbeeld met [Azure Cost Management](#). Dit is een service van Microsoft waarmee je clouduitgaven kunt monitoren, analyseren en beheren. Het geeft inzicht in verbruik per service, project of afdeling en helpt je om

kosten te verdelen en te voorspellen. Voor complexere of hybride-omgevingen bestaan er ook onafhankelijke, gespecialiseerde “FinOps” tools.

Om goed cost management te kunnen inrichten is een aantal zaken belangrijk, namelijk:

- Een heldere tenantstructuur. Volg hiervoor de richtlijnen uit het LCA.
- Gebruik van subscriptions als administratieve eenheid (bijvoorbeeld per omgeving, project afdeling).
- Naming conventions. Door duidelijke namen te geven aan resources kunnen ze makkelijk herkend worden in rapportages.
- Gebruik van tags. Door het instellen van bepaalde policies kan afgedwongen worden om bepaalde tags toe te voegen aan resources. Dit zorgt ervoor dat ze later eenvoudig herleidbaar zijn in kostenrapportages. Denk van tevoren na over de relevante tags ten behoeve van costmanagement bijvoorbeeld ‘owner’, ‘project’, ‘environment’ (prod, acc, test), ‘application’.



Figuur 3 Voorbeeld kosten rapportage