

Handreiking

Gemeentelijke Implementatierichtlijn M365

GGI-Cloud Expertisecentrum

Vereniging van Nederlandse Gemeenten

Nassaulaan 12

2514 JS Den Haag

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

Datum: December 2025

Versie: 1.0

©Vereniging van Nederlandse Gemeenten, Den Haag, december 2025

Inhoudsopgave

Inleiding.....	4
Scope	4
Implementatieadvies.....	5
1. Voer integrale risicoafweging public cloud uit.....	5
2. Voer een data-risicoanalyse en DPIA uit	5
3. M365 omgeving aanvragen.....	5
4. Configureer M365 en gebruik BIO Compliance Initiative Template	6
Privacy vriendelijke instellingen	6
Purview quick wins	6
M365 BIO compliance Initiative template	7
Mapping BIO en template via ISO27002	7
Template downloaden	8
Uitvoeren scripts	8
Resultaten inzichtelijk maken.....	9
Resultaten interpreteren.....	9
Belangrijke punten	11
Planning voor toekomst	11
5. Richt governance in	11

Inleiding

Veel gemeenten nemen hun werkplek af vanuit de cloud. Daarbij is het belangrijk om informatiebeveiliging (IB) en privacybescherming (P) goed te regelen. Immers, ook wanneer de werkplek vanuit de cloud wordt afgenomen geldt dat de gemeente zelf verantwoordelijk is voor een veilige inrichting.

Vrijwel alle gemeente maken gebruik van M365 voor hun werkplek. Het GGI-Cloud Expertisecentrum (GCE) introduceert daarom de gemeentelijke implementatierichtlijn M365. Het doel van de implementatierichtlijn is om ervoor te zorgen dat de configuratie van M365 aan een set minimale IB&P eisen voldoet.

De implementatierichtlijn bestaat naast dit document uit de volgende onderdelen:

- [Integrale Risicoafweging Public Cloud](#)
- [GT Microsoft Framework](#)
- Privacy vriendelijke instellingen
- Purview quick wins
- M365 BIO compliance Initiative template

Scope

Dit document is gericht op de verantwoorde inrichting ten aanzien van IB&P van M365 als technische configuratie. Dit document is geen handleiding voor de inrichting van uw M365 omgeving.

Kern van dit document is het gebruik van het BIO Initiative Policy Template. Daarnaast wordt gerefereerd naar een aantal hulpmiddelen zoals privacyvriendelijke instellingen. Het document gaat niet in op het functioneel inrichten en gebruiken van de onderdelen. De Implementatierichtlijn M365 geeft richtlijnen voor de volgende onderdelen:

- Entra ID (Azure AD)
- Exchange Online
- SharePoint Online
- OneDrive for Business
- Teams
- Purview
- Defender for Office 365
- Ondersteuning voor Intune wordt aan gewerkt

Implementatieadvies

Om een verantwoorde gemeentelijke M365 omgeving in te richten worden in dit document verschillende hulpmiddelen beschreven. 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. Voer een data-risicoanalyse en DPIA uit
3. Vraag de M365 omgeving aan
4. Configureer de M365 omgeving
5. Richt governance in

1. Voer integrale risicoafweging public cloud uit

Voordat een gemeente een Microsoft cloudomgeving 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. 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 omgeving en daarin in te richten onderdelen, met name onderdelen waarbij gemeentelijke data wordt opgeslagen, bewerkt en gedeeld. Gaat het bijvoorbeeld om een Sharepoint- of emailomgeving waarbij géén privacygevoelige data van burgers wordt gedeeld? 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](#).

DPIA herijken

Wanneer een onderdeel dat in de public cloud van Microsoft 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 diverse [generieke DPIA's](#) voor M365 onderdelen hergebruiken. Belangrijk is dat de generieke DPIA gecontroleerd en aangevuld wordt waar nodig. Per individuele gemeente kunnen immers specifieke risico's van toepassing zijn afhankelijk van de door de gemeente gemaakte keuzes. In de generieke DPIA zijn aandachtspunten opgenomen die door uw eigen organisatie nader moeten worden bepaald. In de [Handreiking DPIA voor "Microsoft Teams, OneDrive en SharePoint"](#) wordt dit nader toegelicht.

3. M365 omgeving aanvragen

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

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 diensten en producten. Het advies aan gemeenten is om Microsoft producten en diensten af te nemen onder de voorwaarden van het GT Microsoft Framework.

4. Configureer M365 en gebruik BIO Compliance Initiative Template

Richt de M365 omgeving in met behulp van onderstaande hulpmiddelen:

Privacy vriendelijke instellingen

De [“Handleiding privacyvriendelijke instellingen Microsoft 365 voor beheerders”](#) is een document dat een samenvatting bevat van de privacyadviezen uit de diverse DPIA's voor M365 en wordt beschikbaar gesteld door SLM Rijk. Het beschrijft instellingen die beheerders kunnen doen in een M365 omgeving om deze zo 'privacy vriendelijk' mogelijk in te richten. Het document bestaat uit 24 instellingen. Bij elke instelling wordt aangegeven:

- Waarover gaat het?
- Wat zijn de risico's wanneer deze instellingen niet juist zijn geconfigureerd?
- Een stap-voor-stap handleiding met daarin de acties die nodig zijn om de instellingen juist te configureren.

Het advies is om de instellingen die zijn beschreven in het document over te nemen. Indien dit op een bestaande omgeving gebeurt, dan is het raadzaam om bij elke instelling eerst na te gaan wat de consequenties zijn voor eindgebruikers.

Purview quick wins

Microsoft Purview is een oplossing van Microsoft voor het beveiligen van gegevens in (o.a.) M365. Met Purview is het bijvoorbeeld mogelijk om gegevens te classificeren en op basis van deze classificatie bepaalde regels toe te passen. Purview is bedoeld als centrale plek om inzichtelijk te maken waar bepaalde data zich bevindt, wie er toegang toe heeft en welk beleid (regels) wordt toegepast om deze data te beschermen. De belangrijkste functies zijn:

- Data discovery en classification
Zoekt door bestanden, e-mails, Sharepoint sites etc. en herkent gevoelige data die vervolgens (ook automatisch) gelabeld kan worden met zgn gevoeligheidslabels.
- Data protection (Data Loss Prevention)
Zorgt ervoor dat gevoelige data niet per ongeluk gedeeld kan worden. Iemand kan bijvoorbeeld geen document naar afzenders buiten de gemeente sturen wanneer deze is gelabeld als 'vertrouwelijk'. Ook zorgt data protection voor encryptie van gevoelige data.
- Information Governance & Records Management
Hiermee kun je aangeven wat het retentiebeleid is. Hoelang moet bepaalde data bewaard blijven? Wanneer moeten bestanden verwijderd of gearchiveerd worden?
- Data Map & Data Catalog
Maakt inzichtelijk waar bepaalde data zich bevindt. Bijvoorbeeld in een database, binnen M365, op een lokale server, etc.

Microsoft Purview is beschikbaar met zowel een E3 als een E5 licentie. Het advies is om Purview te gebruiken. Dit kan met minimale configuratie zoals:

- Activeer de default labels
- Pas DLP alvast toe op zeer gevoelige data. Deze categorie is doorgaans al bekend binnen de gemeente
- Beperk de toegang van AI-toepassingen zoals Co-pilot

Vanuit VNG-R gaat het project “Grip op Informatie” veel dieper in op de functionele en

organisatorische kant van de inrichting van informatiebeheer en hoe Microsoft Purview hiervoor ingezet kan worden. Zie: [M365 - Scenario's, praktische antwoorden en tips. Inclusief bijlagen. - KIA community](#)

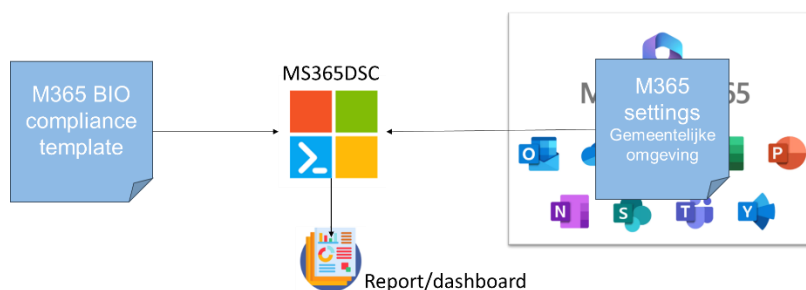
M365 BIO compliance Initiative template

Het “M365 BIO compliance Initiative Template” is sinds september 2025 beschikbaar. Het template met de bijbehorende scripts kan gezien worden als een self-assessment. Door het assessment uit te voeren worden de M365 instellingen van de gemeentelijke omgeving vergeleken met de technische BIO-eisen die zijn opgenomen in het template. De resultaten kunnen worden getoond in een PowerBI dashboard en geven inzicht in hoeverre de omgeving voldoet aan de technische controls uit de BIO. Er wordt niet op alle controls getoetst. Enerzijds komt dit doordat er ook organisatorische controls zijn opgenomen in de BIO waarop niet getoetst kan worden. Anderzijds zijn er ook technische BIO controls die niet verifieerbaar zijn in M365. Het template moet daarom gezien worden als hulpmiddel en goede indicatie om na te gaan in hoeverre een M365 omgeving voldoet aan de BIO. Het is geen garantie.

De technische basis van het template is de technologie:

“[Microsoft 365 Desired State Configuration](#) (M365DSC)”.

De benodigde code en scripts worden aangeboden via [GitHub](#).



Figuur 1: Self-assessment is gebaseerd op MS365DSC

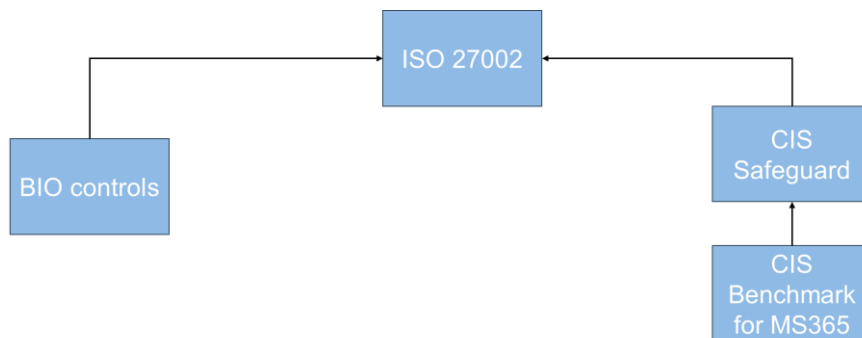
Mapping BIO en template via ISO27002

Het BIO template is niet vanuit een greenfieldsituatie gebouwd maar is gebaseerd op bestaande securitybenchmarks, waarbij is geanalyseerd in hoeverre de controls uit deze benchmarks invulling geven aan de eisen uit de BIO.

De toegepaste benchmarks zijn een aantal Microsoft best practices en de meest essentiële: de CIS benchmark.

Het CIS ([Center of Internet Security](#)) is een non-profit organisatie die voor veel IT producten benchmarks maakt en publiceert. Dit doen ze ook voor M365. De [CIS MS365 benchmark](#) is een internationaal geaccepteerde norm voor een ‘veilige’ M365 omgeving. De CIS MS365 benchmark beschrijft daarvoor een set aan controls (instellingen) waaraan voldaan moet worden. Deze controls zijn door het CIS ook gemapt op zogenaamde CIS SafeGuards. Dit zijn meer algemene veiligheidsmaatregelen. De SafeGuards zijn weer gemapt op ISO27002 controls. Doordat ook veel BIO controls gebaseerd zijn op ISO27002 kan op deze manier een mapping gemaakt worden tussen BIO en relevante M365 instellingen.

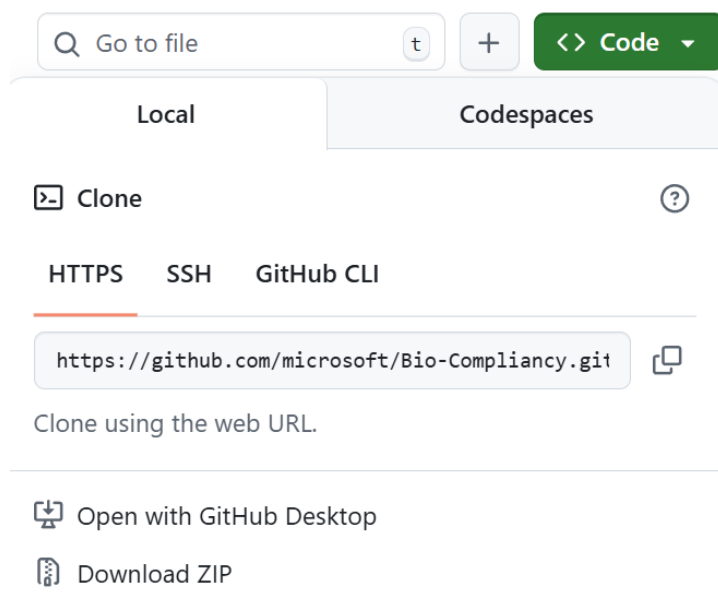
Naast de CIS benchmark is ook een aantal Microsoft best practices toegepast om invulling te geven aan BIO maatregelen.



Figuur 2: Mapping tussen BIO controls en CIS Benchmark

Template downloaden

Het BIO template is beschikbaar via [GitHub](#). Daar is tevens een instructie te vinden hoe u de scripts moet uitvoeren. Je kunt de Github omgeving lokaal klonen of deze als ZIP downloaden. Gebruik daarvoor de groene knop '<> Code' en vervolgens onderaan 'Download ZIP'. Zie Figuur 3.



Figuur 3: Download als ZIP

Wanneer u de Github omgeving lokaal hebt opgeslagen kunt u met de uitvoering van het template beginnen.

Uitvoeren scripts

Het template bestaat uit een aantal PowerShell scripts die de data exporteren en analyseren en een Power BI Dashboard om de resultaten te tonen.

- Het PrepEnvironment script installeert alle benodigdheden
- Het PrepBIOServicePrincipal script maakt een service principal aan in Entra ID. Een service principal is een systeemgebruiker die nodig is om de export te draaien.
- Service principals maken gebruik van sterke authenticatie met een certificaat en maken geen gebruik van MFA. Dit maakt het mogelijk om de export unattended te draaien.
- Het RunBIOExport script maakt een export van alle te evalueren instellingen (in grotere omgevingen kan dit tot enkele uren in beslag nemen).
- Het RunBIOAssessment script vergelijkt de geëxporteerde instellingen met de waardes in de

BIO template en genereert een analyse (in de vorm van een JSON file).

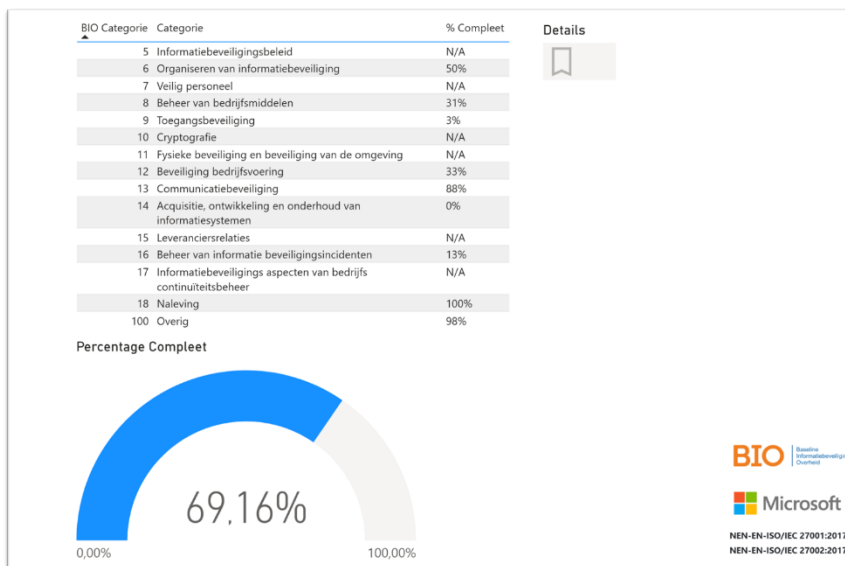
Resultaten inzichtelijk maken

De resultaten kunnen inzichtelijk worden gemaakt via een PowerBI dashboard. Hiervoor is een template (.pbit file) beschikbaar op de Github omgeving.

- Dubbelklik op .pbit file in de Github omgeving
- PowerBI opent en vraagt om locatie van resultaten van analyse
- Selecteer de folder waar het script de resultaten heeft geplaatst (voeg evt. een slash (/) toe aan locatiepad)
- Het dashboard opent

Resultaten interpreteren

Het eerste scherm toont een overzicht van alle BIO controls en in hoeverre de omgeving aan deze controls voldoet. Een score van N/A geeft aan dat hierop niet gecontroleerd is. Er zijn geen CIS controls op deze BIO control te mappen. De laatste categorie (Undocumented unmapped Microsoft 365 Control) is een placeholder voor CIS controls die niet gemapt kunnen worden op een BIO control. Deze controls zijn door CIS dus wel aangemerkt als belangrijk maar hebben geen relatie naar een BIO control.



Figuur 4: Overzicht dashboard BIO controls

Door op een BIO control te klikken (evt. met Ctrl toets) opent een scherm met resultaten voor die specifieke BIO control. Op het scherm staan de subcontrols. Door een specifieke subcontrol te selecteren verschijnen onderin de gerelateerde (gemapte) CIS controls die zijn gebruikt om op deze specifieke BIO subcontrol te toetsen.

161,0 <u>Beheer van informatiebeveiligingsincidenten en -verbeteringen</u>				
BIO Control	Title	% Compleet	Description	BBN
16.1.1	Verantwoordelijkheden en procedures	40%	Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	1
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	N/A	Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	1
16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	0%	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de	1
Totaal		13%		

CIS Control	Title
2.1.3	Ensure notifications for internal users sending malware is Enabled
2.1.6	Ensure Exchange Online Spam Policies are set to notify administrators
5.1.2.5	Ensure the option to remain signed in is hidden
6.1.4	Ensure 'AuditBypassEnabled' is not enabled on mailboxes

Figuur 5: Resultaten specifieke BIO Control

Door te klikken op een specifieke CIS control verschijnen de details.

5.1.2.5 <u>Ensure the option to remain signed in is hidden</u>				
CIS Control Nr CIS Control Title Category Subcategory Level Page Number Required License Rationale 5.1.2.5 Ensure the option to remain signed in is hidden Microsoft Entra admin center Identity 2 156 E3 Allowing users to select this option presents risk, especially if the user signs into their account on a publicly accessible computer/web browser. In this case it would be trivial for an unauthorized person to gain access to any associated cloud data from that account.				
Inventarisatie t.o.v. de baseline				
CIS Control	Instance Naam	Voldoet?	Instelling	Huidige Waarde
5.1.2.5	AADConditionalAccessPolicy-VNG - WebBasedAccessBYOD		DeviceFilterMode	include
5.1.2.5	AADConditionalAccessPolicy-VNG - WebBasedAccessBYOD		DeviceFilterRule	device.trustType -eq 'AzureAD'
5.1.2.5	AADConditionalAccessPolicy-VNG - Web apps - Laptopsgebruikers		DeviceFilterMode	include
5.1.2.5	AADConditionalAccessPolicy-VNG - Web apps - Laptopsgebruikers		DeviceFilterRule	device.trustType -eq 'AzureAD'
5.1.2.5	AADConditionalAccessPolicy-VNG - Systeemaccount WOZ Datacenter		DeviceFilterMode	include
5.1.2.5	AADConditionalAccessPolicy-VNG - Systeemaccount WOZ Datacenter		DeviceFilterRule	device.trustType -eq 'AzureAD'

Figuur 6: Details CIS control

Op de detailpagina van de CIS control is onderaan het scherm een tabel opgenomen of een configuratie-instelling van een instance wel of niet voldoet. Bij elke instelling is aangegeven welke waarde door het script is gevonden en welke waarde de instelling zou moeten hebben om te voldoen aan de control.

Bovenaan het scherm is een beschrijving opgenomen van de CIS control. Deze informatie kunt u gebruiken om in de CIS benchmark de specifieke control op te zoeken en na te gaan welke acties/instellingen nodig zijn om aan deze CIS control te voldoen (zie <https://www.cisecurity.org/cis-benchmarks> klik vervolgens op Microsoft 365, een gratis account is nodig). Wanneer de instellingen zijn aangepast zoals beschreven bij de CIS control, dan zal de score van het template bij een volgende uitvoer verbeteren.

Belangrijke punten

Naast bovenstaande instructie zijn de volgende punten van belang:

- Conditional Access Policy Assignments kunnen niet gechecked worden. Dit moet handmatig gebeuren.
- Het script kan automatisch uitgevoerd worden. Door dit periodiek te doen en de resultaten naar dezelfde folder weg te schrijven kan een 'live dashboard' gemaakt worden.
- PowerBI is gratis beschikbaar. Wanneer een dashboard online te benaderen moet zijn, is een pro licentie nodig. Deze is beschikbaar in E5 of als add-on via E3.
- Problemen met het dashboard kunt u melden bij [GCE](#).
- Voor Microsoft Azure is ook een BIO template beschikbaar op basis van Azure Policy.

Planning voor toekomst

Op dit moment wordt gewerkt aan meerdere verbeteringen van het template namelijk:

- Update naar CIS benchmark 5.0
- Ondersteuning van BIO2/NIS2/Cbw
- Uitbreiding van dashboard met historische data. Hiermee wordt inzichtelijk of de scores verbeteren of juist verslechteren in de tijd.
- Toevoegen van Intune
- Integratie met het Compliance Center in Microsoft 365

5. Richt governance in

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

Wij adviseren gemeenten om het template periodiek uit te voeren en over de resultaten te rapporteren binnen de eigen organisatie.