Strategisch Leveranciersmanagement Microsoft

Ministerie van Justitie en Veiligheid

Rapportage inzake het BIO Compliance Initiative Template voor Microsoft Azure

20 december 2024

Inhoudsopgave

EY Accountants B.V.
Wassenaarseweg 80
2596 CZ Den Haag, Netherlands
Postbus 90636
2509 LP Den Haag, Netherlands

Tel: +31 88 407 10 00
Fax: +31 88 407 41 87
ey.com

VERTROUWELIJK
Ministerie van Justitie en Veiligheid
Strategisch Leveranciersmanagement Microsoft,
Google Cloud en Amazon Web Services

Den Haag, 20 december 2024 BSS0014497/SH/lg

Rapportage onderzoek BIO Compliance Initiative Template

Geachte heer, mevrouw,

U heeft ons een adviesopdracht gegeven tot het onderzoeken van de mate en wijze waarop het BIO Compliance Initiative Template van Microsoft Corporation*, overheidsinstellingen ondersteunt bij het naleven van de BIO-vereisten, welke maatregelen gebruikersorganisaties dienen te treffen om dit template effectief in te kunnen zetten en waar organisaties rekening mee dienen te houden. Conform uw opdracht brengen wij bijgaand onze adviesrapportage uit.

Het concept van deze rapportage is met u en Microsoft Corporation (hierna: Microsoft) afgestemd. De hierbij gemaakte opmerkingen zijn verwerkt in deze definitieve rapportage. Voor de goede orde merken wij op dat dit onderzoek en de hierbij behorende werkzaamheden niet zijn uitgevoerd in het kader van een controle- of beoordelingsopdracht en deze resulteert dan ook niet in een assurance-rapportage.

Wij vertrouwen erop u hiermee van dienst te zijn. Indien u dat wenst zijn wij uiteraard graag bereid tot het geven van een nadere mondelinge toelichting.

Hoogachtend,
EY Accountants B.V.

MAARTEN MUURLING
Digitally signed by MAARTEN MUURLING
DN: cn=MAARTEN MUURLING, c=NL, o=EY Accountants B.V.
Date: 2024.12.20 10:27:30 +01'00'

Maarten Muurling
Partner

1 Inleiding

Als overheden gebruik maken van IT-diensten van derden, dan dienen zij te borgen dat zij bij gebruik van deze IT-diensten voldoen aan de Baseline Informatiebeveiliging Overheid (hierna: BIO). De BIO wordt gehanteerd binnen de Nederlandse overheid; het Rijk, Gemeenten, Waterschappen en Provincies. De BIO betreft één basisniveau voor informatiebeveiliging en één gezamenlijke taal voor alle overheidsorganisaties. De overheid heeft zichzelf verplicht de BIO te implementeren.

Om overheden te ondersteunen bij het voldoen aan de BIO bij het gebruik van Microsoft-producten, is het essentieel dat organisaties binnen de Nederlandse overheid goed geïnformeerd zijn over de mate waarin deze producten voldoen aan de BIO en het bijbehorende Basis Beveiligingsniveau (BBN). Het toegepaste BBN-niveau wordt bepaald op basis van de aard van de data binnen een product. Dit niveau dient als vertrekpunt voor het vaststellen van de te nemen maatregelen. Informatiesystemen en data met een hoger risico en een grotere impact worden geclassificeerd onder een hoger BBN-niveau. De BIO definieert maatregelen op drie BBN-niveaus, afgestemd op verschillende beschermingsniveaus.

BBN1 betreft het basisniveau en richt zich op wat minimaal van de overheid verwacht mag worden voor de bescherming van informatie. Het gaat om een laag betrouwbaarheidsniveau, waarbij uitsluitend de essentiële basismaatregelen worden genomen. Complexe eisen blijven hierbij achterwege.

BBN2 wordt beschouwd als het standaardniveau en is van toepassing op de meeste overheidsinformatie. Dit niveau weerspiegelt goed beheer van informatie, ook wel aangeduid als “goed huisvaderschap”. Het beschermingsniveau binnen BBN2 richt zich op informatie die maximaal de classificatie “Departementaal Vertrouwelijk” (DepV) heeft, zoals gedefinieerd in het VIRBI, of een vergelijkbaar vertrouwelijkheidsniveau bij andere bestuurslagen. Daarnaast valt privacygevoelige informatie met een verhoogd vertrouwelijkheidsniveau binnen dit niveau. Bij dreigingen van statelijke actoren of vergelijkbare dreigingen ligt de nadruk binnen BBN2 op detectiemechanismen. Gemeenten hanteren aanvullend op BBN2 een set maatregelen, bekend als BBN2+, voor informatie met een hoog vertrouwelijkheidsniveau.

BBN3 is bedoeld voor situaties waarin aanvullende maatregelen noodzakelijk zijn om weerstand te bieden tegen statelijke actoren, criminele organisaties of andere complexe dreigingen. Dit niveau geldt ook voor informatie die door de bronhouder een hogere classificatie heeft gekregen dan BBN2. Vanwege de hoge mate van complexiteit schrijft de BIO voor BBN3 geen standaardmaatregelen voor. In plaats daarvan is maatwerk vereist, waarbij bijvoorbeeld gebruik kan worden gemaakt van normenkaders van de NAVO of de Europese Unie.

In deze structuur biedt BBN1 een minimale basis, fungeert BBN2 als standaard, en voorziet BBN3 in bescherming tegen de meest geavanceerde dreigingen.

Zoals in de BIO staat beschreven, vormt BBN2 het uitgangspunt voor informatiesystemen binnen de overheid. In de BIO zijn hiertoe opgenomen:

- BIO-controls (conform de opbouw van ISO-27002/27001).
- BIO-overheidsmaatregelen (specifieke implementatievereisten voor de overheid).

In overeenstemming met de BIO dienen overheden te voldoen aan de in de BIO opgenomen normen, dus zowel de BIO-controls als aan de BIO-overheidsmaatregelen. Voor de normen waaraan (nog) niet (volledig) kan worden voldaan, dient te worden uitgelegd hoe met het risico van het niet voldoen aan deze normen wordt omgegaan (comply or explain). Ook dienen organisaties conform de BIO eventuele risico's inzichtelijk te maken.

Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services (hierna: SLM), onderdeel van het Ministerie van Justitie en Veiligheid, ontzorgt overheden door onderzoeken te laten uitvoeren naar de beveiliging en privacy bij de inzet van Hyperscalers. Hyperscalers zijn de grote cloudserviceproviders, waaronder Amazon Web Services (AWS), Microsoft Azure en Google Cloud.
SLM laat hierbij onderzoek uitvoeren in het kader van:

- DPIA's
- (Technische) verificatieonderzoeken
- Audits

Kenmerkend voor deze onderzoeken en audits is dat bij Hyperscalers "onder de motorkap" onderzoek kan plaatsvinden.

Het voorliggende rapport betreft een onderzoek naar de mate waarin het "BIO Compliance Initiative Template"[1], ontwikkeld door Microsoft, overheden kan ontzorgen bij het voldoen aan de BIO (en bijbehorende BBN-niveau's) op het moment dat zij Microsoft Azure producten afnemen.
Hiervoor hebben wij de reikwijde, werking en beperkingen van het BIO Compliance Initiative Template geëvalueerd.

1 Dit betreft het template, zoals opgesteld door Microsoft, en beschikbaar is gesteld via Github: https://github.com/Azure/Bio-Compliancy

2 Opdracht

In dit hoofdstuk is de onderliggende vraagstelling, doelstelling en reikwijdte van het door ons uitgevoerde onderzoek beschreven. Dit inclusief de uitgangspunten en de beperkingen.

2.1 Onderliggende vraagstelling

SLM heeft EY gevraagd een onderzoek uit te voeren naar de volgende vraag:

> *"In hoeverre en op welke wijze (met welke maatregelen aan de gebruikerszijde) is bij het toepassen van het BIO Compliance Initiative Template, Microsoft Azure door een gebruikersorganisatie BIO-compliant te gebruiken?"*

2.2 Doelstelling van de opdracht

Het BIO Compliance Initiative Template is een door Microsoft aangeboden oplossing voor het monitoren van diverse systeem/beveiligingsinstellingen binnen Microsoft Azure. Middels het template kan een gebruikersorganisatie inzicht krijgen in de mate waarin bepaalde instellingen in lijn zijn met de vereisten vanuit de BIO. Het template dwingt dus geen instellingen af, maar monitort deze. Ons onderzoek heeft als doel om te bepalen in welke mate en op welke wijze het BIO Compliance Initiative Template overheidsinstellingen ondersteunt bij het naleven van de BIO-vereisten.

2.3 Reikwijdte en afbakening

Het template van Microsoft monitort een verscheidenheid aan instellingen binnen Microsoft Azure, inclusief instellingen die betrekking hebben op niet-BIO-gerelateerde normen. De reikwijdte van ons onderzoek omvat de BIO-normen die volgens Microsoft in het BIO Compliance Initiative Template worden geraakt. Hierbij spreken wij van geraakt, aangezien de volledige beschrijving van BIO-normen niet 1:1 technisch worden gemonitord. Dit template van Microsoft monitort een verscheidenheid aan instellingen binnen Microsoft Azure, inclusief instellingen die betrekking hebben op niet-BIO-gerelateerde normen. Ons onderzoek is afgebakend tot de monitoring van systeeminstellingen binnen het BIO Compliance Initiative Template die een raakvlak hebben met BIO-controls en overheidsmaatregelen.

2.4 Uitgangspunten

Het BIO Compliance Initiative Template wordt doorlopend door Microsoft gewijzigd en vernieuwd. Dit betreft onder meer het toevoegen of verwijderen van monitoringsmogelijkheden van systeeminstellingen. Het door ons uitgevoerde onderzoek heeft betrekking op de basisversie 2.3.3 van het template. Ook hebben wij de BIO als referentie gebruikt voor ons onderzoek. Dit betrof versie 1.04 van de BIO.

2.5 Beperkingen

De door ons geleverde dienstverlening en dit rapport is adviserend van aard en betreft geen controle, beoordeling of andersoortige assurance-opdracht overeenkomstig controle- en assurance-standaarden zoals uitgevaardigd door de Nederlandse Beroepsorganisatie van Accountants (NBA) of de International Auditing and Assurance Standards Board en vergelijkbare organisaties. Wij verstrekken derhalve geen enkele vorm van assurance.

De volgende werkzaamheden maken dan ook geen onderdeel uit van ons onderzoek:

- Het geven van een oordeel over de volledige (technische-)werking van het BIO Compliance Initiative Template. Als onderdeel van het onderzoek hebben wij slechts de monitoring van een aantal systeeminstellingen beoordeeld voor het vaststellen van de werking.
- Het geven van een oordeel over de werking van systeeminstellingen binnen Microsoft Azure. Als onderdeel van ons onderzoek heeft enkel een beoordeling plaatsgevonden op de werking van de monitoring op systeeminstellingen.
- Het geven van een oordeel over de juistheid van de door Microsoft gemaakte koppeling tussen de gemonitorde systeeminstellingen en de gerelateerde BIO-normen.

Gebruik van de rapportage

De beoogde gebruikers van deze rapportage zijn Nederlandse overheidsorganisaties die gebruik maken van Microsoft Azure en verplicht zijn de BIO toe te passen (en onder de MBSA[2] tussen SLM Rijk en Microsoft vallen). Het doel van het door ons uitgevoerde onderzoek is het geven van inzicht over de mate waarin het BIO Compliance Initiative Template Nederlandse overheidsorganisaties kan ondersteunen bij het voldoen aan de BIO.

Deze rapportage, onze beschrijving van werkzaamheden en resultaten mogen enkel door de beoogde gebruikers worden gebruikt voor het doel waarvoor deze is opgesteld en dient niet te worden gebruikt door anderen.

Onze rapportage mag alleen in zijn geheel beschikbaar worden gesteld aan de beoogde gebruikers. Zonder onze voorafgaande schriftelijke toestemming, mogen onze rapportage, onze beschrijving van werkzaamheden en resultaten niet gedeeltelijk worden verspreid of verstrekt aan anderen. Tevens mag u niet zonder onze voorafgaande schriftelijke toestemming uit onze rapportage, onze beschrijving van werkzaamheden en resultaten citeren of laten citeren.

2 MBSA: Rijksbrede Microsoft Business and Services Agreements

3 Werkwijze

3.1 Organisatie

Bij het uitvoeren van deze opdracht zijn de stakeholders Microsoft en SLM betrokken geweest. Vanuit Microsoft zijn ontwikkelaars en architecten betrokken voor het toelichten en aantonen van de inhoud en werking van het BIO Compliance Initiative Template. Daarnaast hebben wij in afstemming met Microsoft, als onderdeel van fase B van dit onderzoek, een review uitgevoerd op de door het BIO Compliance Initiative Template geraakte BIO controls en overheidsmaatregelen. SLM heeft in afstemming met Microsoft en EY de scope van fase C bepaald.

3.2 Aanpak

Voor het beantwoorden van de onderzoeksvraag en het behalen van de doelstellingen is dit onderzoek uitgevoerd in drie fasen:

Fase	Beschrijving
A. Review opzet BIO Compliance Initiative Template	In fase A is de algemene werking van het BIO Compliance Initiative Template onderzocht, waarin: • inzicht is verkregen in de totstandkoming en werking van het template; • wat de relatie is met de BIO-controls en overheidsmaatregelen; • inzicht verkregen in de door het template gemonitorde systeeminstellingen.
B. Review scope BIO Compliance Initiative Template	In fase B is de scope aan BIO-normen onderzocht die door het template worden geraakt. Wij hebben in fase B onderzocht welke van deze (honderden) gemonitorde systeeminstellingen gerelateerd zijn aan een BIO-control of overheidsmaatregel.
C. Review monitoring en randvoorwaarden BIO Compliance Initiative Template	In fase C is de werking en randvoorwaarden van het BIO Compliance Initiative Template onderzocht. Hierin zijn, in overleg met SLM, een aantal systeeminstellingen geselecteerd en is in een nieuw ingerichte Azure-omgeving (specifiek een Sovereign Landing Zone) bepaald of monitoring systeemtechnisch is ingericht en welke aandachtspunten hierbij ontstaan. Daarnaast zijn de randvoorwaarden inzichtelijk gemaakt die benodigd zijn voor het effectief inrichten en gebruiken van het template.

Dit rapport bevat de uitkomsten van de fasen A, B en C.

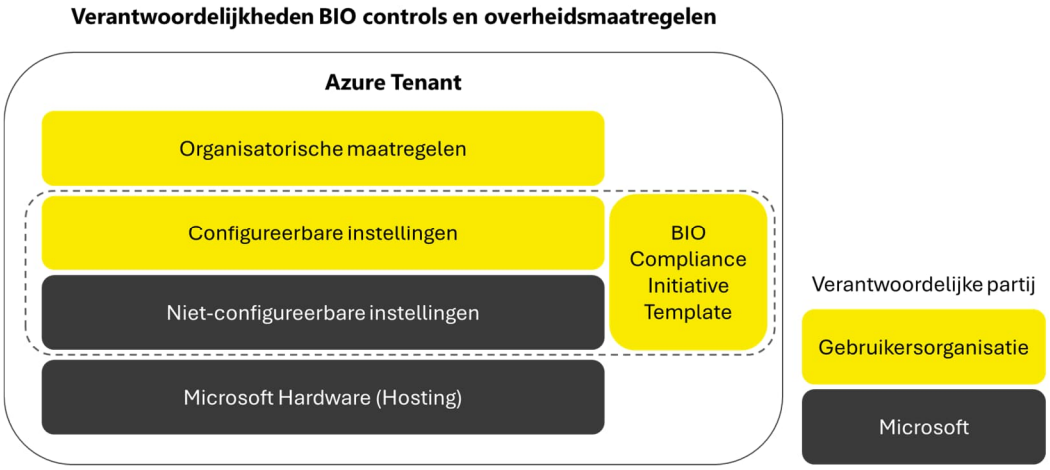
4 Managementsamenvatting

Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services (hierna: SLM) heeft EY gevraagd een onderzoek uit te voeren inzake Microsoft betreffende de volgende vraag:

> *"In hoeverre en op welke wijze (met welke maatregelen aan de gebruikerszijde) is bij het toepassen van het BIO Compliance Initiative Template, Microsoft Azure door een gebruikersorganisatie BIO-compliant te gebruiken?"*

Om de onderzoeksvraag te beantwoorden, hebben wij drie fasen doorlopen om de opzet, scope en werking van het BIO Compliance Initiative Template vast te stellen. De uitkomsten van ons onderzoek geeft antwoord op de hoofdvraag en biedt gebruikersorganisaties concrete handvatten voor een zorgvuldige implementatie en gebruik van het BIO Compliance Initiative Template.

Wij hebben geconstateerd dat het template bestaat uit een monitoringsoplossing (security policy) die gebruikersorganisaties kunnen toepassen op hun Azure-omgeving. Het template controleert of de systeeminstellingen binnen Azure in overeenstemming zijn met de Best Practices van Microsoft, zonder deze instellingen af te dwingen. De verantwoordelijkheid voor een juiste en veilige configuratie van de Azure Tenant is en blijft bij de gebruikersorganisaties liggen. Wij hebben eveneens geconstateerd dat het BIO Compliance Initiative Template zowel configureerbare als niet-configureerbare instellingen binnen Azure monitort. Daarnaast is monitoring enkel actief op Azure Workloads (Resources binnen de Azure Public Cloud). Microsoft producten zoals M365, Azure DevOps en Dynamics CRM, et cetera worden dus niet gemonitord door deze template. Afbeelding 1 toont de lagen binnen de Azure Tenant waarop het template actief is. Hierbij is ook visueel gemaakt waar de verantwoordelijkheid ligt voor het implementeren van maatregelen in lijn met de BIO-normen. Ten aanzien van de Hosting van Azure en relevante BIO controls en overheidsmaatregelen verwijzen wij naar ons onderzoek van 20 oktober 2023 "Onderzoek BIO Compliant gebruik Microsoft"[3]. Dit betreft het onderzoek van de mate van compliance van Microsoftdiensten in relatie tot de BIO, op basis van reeds aanwezige assurance rapportages over deze diensten.



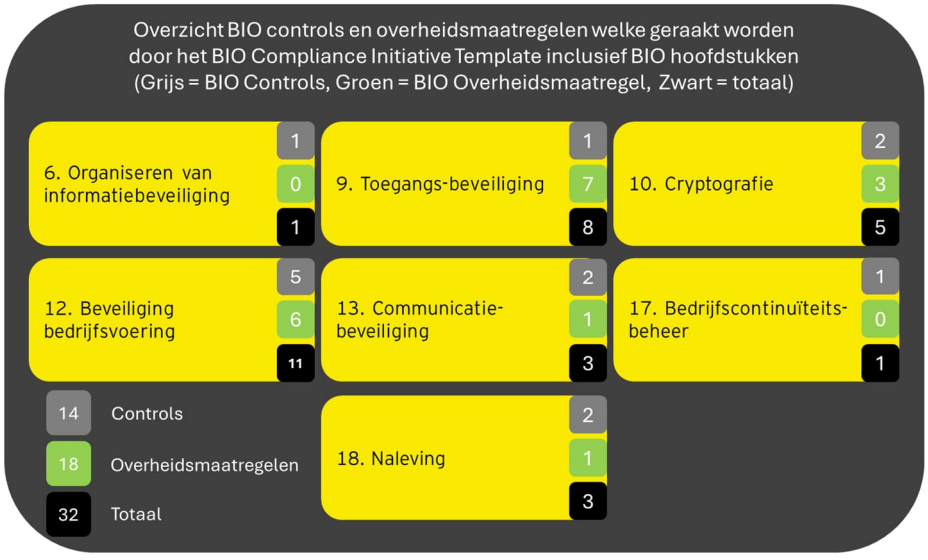
Afbeelding 1: Overzicht scope en verantwoordelijkheden bij het inzetten het BIO Compliance Initiative Template

3 Https://slmmicrosoftrijk.nl/wp-content/uploads/2023/11/REQ6802038-21-MinJenV-Rapportage-Onderzoek-BIO-fase-A-en-B-20-10-2023.pdf

Het BIO Compliance Initiative Template is gebaseerd op de BIO Thema-uitwerking Clouddiensten in plaats van de BIO zelf. Deze thema-uitwerking is een door het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) ontwikkelde handreiking voor organisaties die clouddiensten gebruiken of van plan zijn dit te doen. Doordat de inrichting van het template is ingericht aan de hand van deze handreiking is het voor gebruikersorganisaties niet eenduidig te bepalen welke BIO-controls en overheidsmaatregelen door het template worden geraakt. Om deze reden hebben wij een matrix opgesteld waarin relaties inzichtelijk zijn gemaakt tussen de gemonitorde instellingen en de bijbehorende BIO-controls en overheidsmaatregelen. Voor het opstellen van deze matrix hebben wij allereerst per BIO-norm beoordeeld in hoeverre deze betrekking heeft op een technische Cloud inrichting. Wij hebben beoordeeld dat van de 250 BIO-normen (Controls en Overheidsmaatregelen) voor 65 normen een technisch element aanwezig is met betrekking tot IaaS en PaaS oplossingen. Wij hebben als resultaat van ons onderzoek bepaald dat 32 van deze 65 BIO-normen worden geraakt door het BIO Compliance Initiative Template.Afbeelding 2 biedt een overzicht van de 32 in-scope BIO-controls en overheidsmaatregelen per hoofdstuk vanuit de BIO (waaronder per hoofdstuk het aantal controls, overheidsmaatregelen en het totaal). Voor een samenvatting van de monitoring per BIO-control of overheidsmaatregel verwijzen wij naar bijlage 2.

Aandachtspunt

Wij attenderen gebruikersorganisaties erop dat de compliance statussen in het BIO Compliance Initiative Template zijn gebaseerd op Microsoft Best Practices (Microsoft Cloud Security Benchmark), die zijn gekoppeld aan BIO controls en overheidsmaatregelen. Aangezien per control of maatregel mogelijk in meer of mindere mate wordt gemonitord dan vereist vanuit de BIO, adviseren wij gebruikersorganisaties om: (1) het toepasselijke BBN-niveau vast te stellen op basis van de data en informatiesystemen op het Azure-platform, (2) de systeemtechnische elementen te beoordelen op voldoende naleving van zowel de BIO als interne beleidsvereisten, en (3) het overzicht van Microsoft met daarin de koppeling tussen instellingen en BIO controls en overheidsmaatregelen regelmatig te evalueren, aangezien updates aan het template wijzigingen in dit overzicht kunnen veroorzaken.



Afbeelding 2: BIO Compliance Initiative Template - in scope BIO controle en overheidsmaatregelen

Om de werking van monitoring door het template te beoordelen hebben wij voor drie systeeminstellingen die in het template ingesteld staan, validatiewerkzaamheden uitgevoerd. Wij hebben voor deze instellingen vastgesteld dat het template de compliant status correct weergeeft volgens de geconfigureerde systeeminstellingen en dat bij wijzigingen in de systeeminstellingen de compliant status van het template overeenkomstig wordt aangepast.

Aandachtspunt 

Tot slot hebben wij een aantal belangrijke randvoorwaarden voor gebruikersorganisaties geïdentificeerd voor het versterken van de betrouwbaarheid van monitoring, te weten:

Randvoorwaarden	Details
Logging inschakelen	Gebruikersorganisaties dienen logging in te schakelen van meldingen (monitoring van de “compliant” statussen) en wijzigingen aan het template, om een audittrail van BIO compliancy te waarborgen en ongeautoriseerde aanpassingen te detecteren.
Periodieke controles/ Automatische alarmering	Gebruikersorganisaties dienen periodieke controles of automatische alarmering in te stellen voor tijdige opvolging van meldingen van het template.
Formeel change proces	Gebruikersorganisaties dienen wijzigingen aan het template via een formeel change proces te laten voorlopen.
Autorisatiebeheer	Gebruikersorganisaties dienen bij de inzet van het template, na te gaan of het template op management group- of subscriptieniveau wordt ingezet en welke gebruikers verantwoordelijk zijn voor het beheer van het template.
Functiescheiding	Gebruikersorganisaties dienen functiescheiding te waarborgen tussen IT- en template-beheerders voor het voorkomen van ongeautoriseerde wijzigingen.

Deze randvoorwaarden moeten gebruikersorganisaties (overheidsinstellingen) gedegen implementeren om optimaal gebruik te kunnen maken van het BIO-template.

Conclusie hoofdvraag
Het onderzoek toont aan dat het BIO Compliance Initiative Template een waardevol hulpmiddel kan zijn voor het monitoren van een Azure-omgeving op instellingen die bijdragen aan een BIO-compliant inrichting. Het template biedt uitgebreide monitoring van systeeminstellingen, controleert of deze instellingen voldoen aan de Microsoft Best Practices (Microsoft Cloud Security Benchmark), en relateert deze aan diverse BIO-normen met een technisch cloudcomponent. Dit helpt gebruikers inzicht te krijgen in de mate waarin hun Azure-omgeving voldoet aan de BIO-normen. Het is echter belangrijk om te onderstrepen dat het template slechts een hulpmiddel is en geen volledige BIO-compliancy garandeert. Het template biedt ondersteuning bij het voldoen aan 32 BIO-normen. Gebruikersorganisaties dienen zelf aanvullende (organisatorische en technische) maatregelen te treffen en beoordelen of de Microsoft Best Practices overeenkomen met het interne geldende beleid en specifieke eisen in de BIO-normen.
Omdat veel BIO-normen maatwerk vereisen op basis van organisatiebeleid, kan het template enkel effectief zijn als dit beleid aansluit op de gehanteerde configuraties.

5 Uitkomsten onderzoek

Op basis van de door ons uitgevoerde werkzaamheden zijn in dit hoofdstuk de detailresultaten per fase uiteengezet. Het doorlopen van de onderzoeksfasen heeft geleid tot beantwoording van de hoofdvraag en onze belangrijkste constateringen zoals deze zijn opgenomen in de managementsamenvatting.
In dit hoofdstuk lichten wij onze werkzaamheden inclusief de uitkomsten toe.

5.1 Fase A: Review opzet BIO Compliance Initiative Template

Als onderdeel van fase A hebben wij onderzoek uitgevoerd naar de opzet en algemene werking van het BIO Compliance Initiative Template.

5.1.1 Inleiding

Het BIO Compliance Initiative Template is een hulpmiddel dat als policy kan worden ingeladen in een Microsoft Azure-omgeving. In combinatie met Defender for Cloud stelt dit template gebruikersorganisaties in staat de systeeminrichting en instellingen binnen de omgeving te monitoren op conformiteit met de BIO. Het template geeft hierbij de mogelijkheid monitoring aan te passen naar de wensen en eisen van de gebruikersorganisatie. Gebruikersorganisaties kunnen hierbij zelf de scope van monitoring bepalen, denk hierbij aan het toewijzen van het template op specifieke Azure Subscripties of het uitschakelen van monitoring op specifieke Azure Resources. Het template richt zich uitsluitend op de in de BIO opgenomen technische normen, waarbij aanvullende procesmatige normen door de organisatie zelf moeten worden ingevoerd om volledige BIO-compliant te worden. Daarnaast is monitoring enkel actief op Azure Workloads (Resources binnen de Azure Public Cloud). Microsoft producten zoals M365, Azure DevOps en Dynamics CRM, et cetera worden dus niet gemonitord door het template. In totaal kunnen er 261 systeeminstellingen worden gemonitord door het Template. Deze systeeminstellingen zijn te relateren aan diverse BIO-controls en overheidsmaatregelen.

Wij merken op dat Microsoft een algemene disclaimer heeft opgesteld voor het gebruik van het template (https://github.com/Azure/Bio-Compliancy):

“Deze BIO template dient te worden gezien als hulpmiddel om BIO compliancy te bereiken en is gericht op het beoordelen van de technische configuratie van Azure workloads. Onder geen enkele voorwaarde garandeert Microsoft dat deze template direct leidt tot een volledige BIO compliancy ten aanzien van resources in de Microsoft Azure omgeving. Ook dienen processen ingericht te zijn binnen de organisatie om administratieve processen te borgen ten aanzien van de BIO.”

Daarnaast willen wij benadrukken dat de monitoring van het template gebaseerd is op de Microsoft Cloud Security Benchmark[4]. De gebruikersorganisatie dient zelf na te gaan in hoeverre de door Microsoft aanbevolen inrichting en instellingen in lijn zijn met de BIO en haar interne processen. De Microsoft Cloud Security Benchmark (MCSB) is een set van best practices en aanbevelingen die organisaties helpt bij het beveiligen van hun cloudomgevingen in Microsoft Azure. De benchmark is gebaseerd op internationale standaarden zoals het CIS-framework, NIST, en de PCI. Ook bestaat de MCSB uit controls afkomstig van de Azure Security Benchmark, een door Microsoft zelf ontwikkelde standaard die specifiek is afgestemd op Azure-cloudservices.

[4] Zie: https://learn.microsoft.com/en-us/security/benchmark/azure/introduction

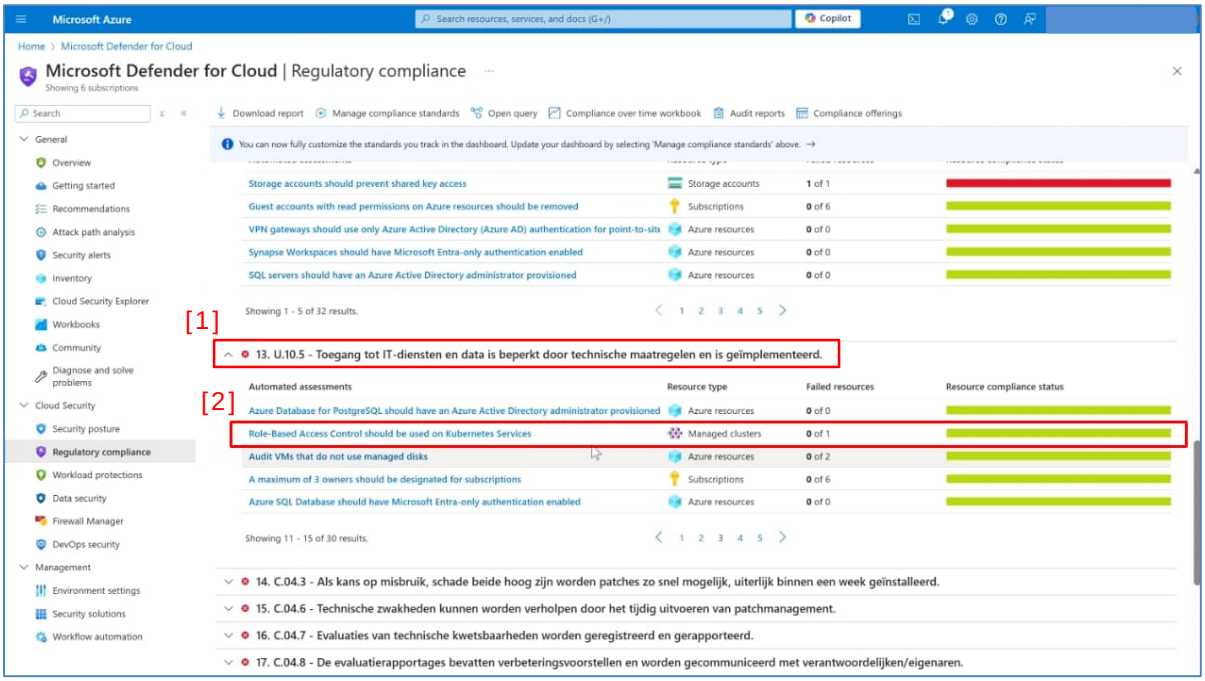
Gebruikers kunnen het template vanuit de Microsoft Github pagina importeren naar de Azure-omgeving waarop zij monitoring willen toepassen. Vanuit Github wordt het template toegevoegd aan de Security Policies binnen Defender for Cloud[5]. Naast implementatie via Github is er ook een Builtin variant beschikbaar. Dit betreft een standaard ingeladen policy in de Azure-omgeving die door gebruikers-organisaties kan worden ingeschakeld en betreft een Engelstalige versie. Gebruikersorganisaties kunnen het template zowel op management group niveau toekennen als op subscriptieniveau. Op management group niveau kunnen de configuraties van het template (zoals filteringen en instellingen) gewijzigd worden door de root-user. Indien het template op subscriptie niveau is toegekend kunnen ook geautoriseerde subscriptie owners wijzigingen aanbrengen. Daarnaast kan de gebruikersorganisatie ervoor kiezen om separaat autorisaties toe te kennen aan gebruikers binnen Azure voor het maken van wijzigen aan het template.

5.1.2 Algemene werking

Het template monitort of de systeeminrichting en instellingen die een gebruikersorganisatie in Azure heeft ingeregeld voldoen aan de BIO controls en overheidsmaatregelen. Belangrijk om te benoemen is dat het template ten tijde van ons onderzoek geen mogelijkheid bood voor het doorvoeren of afdwingen van configuraties in de Azure-omgeving conform BIO-vereisten. Daarnaast is het BIO Compliance Initiative Template ingericht en weergegeven (in de naamvoering) op basis van thema's vanuit de handreiking "BIO Cloud Thema-uitwerking" (https://cip-overheid.nl/media/h4lcnhdn/20230322-bio-thema-uitwerking-clouddiensten-v22-def.pdf), die door het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) is opgesteld. Deze Thema-uitwerking bevat een subset aan BIO-controls en overheidsmaatregelen. Dit wordt nader toegelicht in 5.1.4 BIO Cloud Thema-uitwerking.

Om een beeld te geven op welke wijze het template compliance op basis van BIO weergeeft in Microsoft Azure Defender for Cloud is hieronder een afbeelding bijgevoegd (zie afbeelding 3). Ter illustratie hebben wij de monitoring op de instellingen als onderdeel van de BIO Cloud Thema-uitwerking thema: "U10.5 – Toegang tot IT-diensten en data is beperkt door technische maatregelen en is geïmplementeerd" geopend [1]. Het BIO Compliance Initiative Template zien dat Role-based Control als onderdeel van de vereiste maatregelen is ingeschakeld voor Kubernetes Services [2] (Resource Compliance Status = groen).

5 Belangrijke randvoorwaarde hierbij is dat gebruikersorganisaties "Defender for Servers" of 'Defender CPSM' ingeschakeld hebben.



Afbeelding 3: Schermprint BIO Compliance Initiative Template – Monitoring op Role-Based Access in Kubernetes

Aandachtspunt

Naast de wijze waarop het BIO Compliance Initiative Template wordt weergegeven zijn er een aantal belangrijke aandachtspunten in de werking en gebruik:

5.1.2.1 Aandachtspunt 1: geen real-time monitoring

Het BIO Compliance Initiative Template monitort systeeminstellingen niet real-time. De verversings-frequentie (refresh rate) is afhankelijk van Defender for Cloud en kan verschillen per Azure-resource. Zo worden systeeminstellingen gerelateerd aan securityinstellingen veelal éénmaal per dag ververst.

5.1.2.2 Aandachtspunt 2: Multicloud vs Hybrid Cloud

Wanneer een organisatie een Multi-Cloud of Hybrid-Cloud strategie hanteert, is het mogelijk om het BIO Compliance Initiative Template ook in te zetten voor resources die zich bevinden in een Private Cloud of bij andere Cloud providers, zoals Google Cloud of Amazon Web Services (AWS). Dit biedt flexibiliteit om het template breder toe te passen buiten de Microsoft Azure-omgeving. Het is echter belangrijk dat deze externe resources toegankelijk zijn voor Microsoft Defender for Cloud, zodat Defender for Cloud de benodigde gegevens kan uitlezen en monitoren. Zonder deze toegang is het niet mogelijk om de compliance van deze resources te beoordelen met behulp van het template. De toegang dient specifiek te worden toegewezen door de betreffende organisaties.

5.1.2.3 Aandachtspunt 3: Template houdt rekening met niet configureerbare systeeminstellingen

Het BIO Compliance Initiative Template houdt tevens rekening met niet-configureerbare instellingen, oftewel instellingen die van nature compliant zijn met het template. Dit betekent dat het template bepaalde instellingen bewaakt die niet kunnen worden gewijzigd naar een “niet-compliant” status. Deze instellingen zijn technisch zo afgedwongen dat ze altijd voldoen aan de vereiste compliance-normen, oftewel Microsoft Cloud Security Benchmark controls. De gebruikersorganisatie krijgt hierdoor tevens inzicht in welke mate niet-configureerbare systeeminstellingen aanwezig zijn die de organisatie ondersteunt bij het BIO compliant zijn.

Een voorbeeld hiervan is indien een gebruikersorganisaties een Sovereign Cloud Landing Zone heeft ingericht. Als onderdeel van deze landingzone is systeemtechnisch vastgelegd dat geen datacenters buiten de EU gebruikt kunnen worden. Hierdoor is het niet mogelijk om een “niet-compliant” status te genereren binnen het BIO Compliance Initiative Template, aangezien deze instelling altijd aan de BIO-vereisten voldoet zonder dat wijzigingen nodig zijn. Het is aan te raden voor gebruikersorganisaties periodiek te controleren of deze systeeminstellingen gedurende gebruik van Azure producten niet-configureerbaar blijven.

5.1.3 Sovereign Landing Zone & BIO Compliance Initiative Template

Gebruikersorganisaties die gebruik maken van Microsoft Azure hebben de mogelijkheid om Azure Landing Zones te implementeren. Een Landing Zone is een vooraf geconfigureerde inrichting van cloudinfrastructuur waarop organisaties applicaties en workloads eenvoudig kunnen implementeren en beheren. Dit biedt gebruikersorganisaties het gemak van een voorgedefinieerde infrastructuur die direct in gebruik kan worden genomen. Afhankelijk van het type organisatie kan worden gekozen voor verschillende soorten Landing Zones. Speciaal voor overheidsinstellingen heeft Microsoft de “Sovereign Landing Zone” (SLZ) ontwikkeld.

De SLZ is een variant van de enterprise-scale Azure Landing Zone, ontworpen voor overheidsorganisaties die behoefte hebben aan strengere controle op soevereiniteit (https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/). Microsoft geeft aan dat de SLZ organisaties ondersteunt in het voldoen aan regelgevingseisen, zoals de BIO, door gebruik te maken van Azure-native mogelijkheden zoals Infrastructure-as-Code (IaC) en Policy-as-Code (PaC). Bij het gebruik van een SLZ worden standaard infrastructuurconfiguraties en Azure Policies afgedwongen. Het zelf inrichten van de Azure-omgeving conform het BIO Compliance Initiative Template kan complex zijn. Volgens Microsoft wordt middels een SLZ “by design” de Azure inrichting en instellingen conform de Microsoft Cloud Security Benchmark, zoals opgenomen in het template, ingericht. Het is aan te raden voor gebruikersorganisatie, bij het inzetten van een landingzone, kritisch in acht te nemen welke onderdelen worden afgedwongen en in hoeverre monitoring daarop mogelijk is. Dit beperkt het risico op de aanwezigheid van workloads die niet voldoen aan de BIO. Het gebruik en validatie van deze landingzone is geen onderdeel geweest van dit onderzoek.

5.1.4 BIO Cloud Thema-uitwerking (Het template in relatie tot BIO controls en overheidsmaatregelen)

Op basis van ons onderzoek hebben wij vastgesteld dat het BIO Compliance Initiative Template is gebaseerd op en ingericht volgens de BIO Thema-uitwerking Clouddiensten (hierna: thema-uitwerking), en niet direct op de BIO-normen. Deze thema-uitwerking is een door het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) ontwikkelde handreiking voor organisaties die clouddiensten gebruiken of van plan zijn dit te doen. Voor meer informatie verwijzen wij naar https://cip-overheid.nl/productcategorieen-en-workshops/producten?product=Clouddiensten.

In relatie tot de BIO zijn binnen de thema-uitwerking slechts 21 van de 250 BIO controls en overheidsmaatregelen aanwezig. Naast controls en overheidsmaatregelen afkomstig uit de BIO bevat de thema-uitwerking ook controls uit overige standaarden, zoals het Cybersecurity Framework (CSW), Cloud Control Matrix (CCM), Standard of Good Practice (SoGP) 2018 et cetera Voor de gebruikersorganisatie is het dus belangrijk te weten dat de huidige inrichting van de BIO Compliance Initiative Template(instellingen) gekoppeld is aan de thema's en onderliggende controls binnen de thema-uitwerking en niet rechtstreeks gekoppeld aan BIO-normen. Ter referentie verwijzen wij naar afbeelding 3, waarin zichtbaar is dat meerderde systeeminstellingen gekoppeld zijn aan een Cloud thema (U10.5 – Toegang tot IT-diensten en data is beperkt door technische maatregelen en is geïmplementeerd).

Om bovenstaande reden hebben wij in dit onderzoek een overzicht gecreëerd van de door de BIO Compliance Initiative Template gemonitorde instellingen in relatie tot de BIO-normen, zie hiervoor tabel 5 in bijlage 1. Op deze wijze is voor de gebruikersorganisatie inzichtelijk welke BIO controls en overheidsmaatregelen geraakt worden door het BIO Compliance Initiative Template en daarbij mogelijk de gebruikersorganisatie kan ondersteunen bij het naleven van de BIO.

5.2 Fase B: Review scope BIO Compliance Initiative Template

Zoals in sectie 5.1.4 beschreven is de inrichting van het template gebaseerd op de “Cloud Thema Uitwerking”, waarbij gemonitorde instellingen zijn gekoppeld aan een “Cloud Thema” in plaats van een BIO-control of -overheidsmaatregel. In fase B hebben wij onderzocht welk BIO-controls en -overheidsmaatregelen geraakt worden door het BIO Compliance Initiative Template en daarmee de reikwijdte op de BIO van het template bepaald. Wij hebben in dit hoofdstuk bepaald welke van deze gemonitorde systeeminstellingen gerelateerd zijn aan een BIO-control en -overheidsmaatregel. Op deze wijze is het voor de gebruikersorganisatie inzichtelijk met welke BIO controls en overheidsmaatregelen het template ondersteunt in de monitoring op naleving.

5.2.1 Technische vs niet-technische BIO-controls en -overheidsmaatregelen

De BIO betreft een normenkader van 250 controls en overheidsmaatregelen die variëren van organisatorische maatregelen, zoals procedures en beleid, tot technische maatregelen, zoals encryptiestandaarden. Allereerst hebben wij per BIO-control en -overheidsmaatregel onderzocht in hoeverre de control of overheidsmaatregel een technisch component bevat die binnen een IaaS- en PaaS-inrichting zou kunnen worden gemonitord. Van de 250 normen zijn voor 65 controls en overheidsmaatregelen een technisch element aanwezig met betrekking tot IaaS en PaaS oplossingen. Van deze 65 worden 32 controls en overheidsmaatregelen geraakt door het BIO Compliance Initiative Template. In bijlage 1 tabel 5 is het overzicht opgenomen van de Cloud gerelateerde BIO controls en overheidsmaatregelen. In tabel 1 is een overzicht aan totalen opgenomen.

Tabel 1: Overzicht BIO Controls en overheidsmaatregelen met technisch IaaS/PaaS element

Overzicht	Totaal	Controls	Overheids-maatregelen
Totalen			
BIO controls en overheidsmaatregelen	250	112	138
BIO-normen met technisch Cloud element			
BIO controls en overheidsmaatregelen zonder technisch Cloud element	185	77	108
BIO controls en overheidsmaatregelen met technisch Cloud element	65	35	30
BIO-normen aanwezig in het BIO Compliance Initiative Template			
BIO controls en overheidsmaatregelen aanwezig in BIO Compliance Initiative Template	32 ✓	14 ✓	18 ✓
BIO Controls en overheidsmaatregelen niet aanwezig in BIO Compliance Initiative Template	33×	21 ×	12 ×

5.2.2 Overzicht 32 BIO controls en overheidsmaatregelen die geraakt worden door het BIO Compliance Initiative Template

De in het BIO Compliance Initiative Template gemonitorde instellingen zijn gekoppeld aan 32 BIO controls en overheidsmaatregelen. Met andere woorden zijn ten aanzien van 32 BIO controls en overheidsmaatregelen Microsoft Best Practices waarop het template monitort of instellingen conform deze best practices zijn geconfigureerd. Voor elk van deze BIO controls en overheidsmaatregelen hebben wij samengevat welke systeeminstellingen door het template worden gemonitord, inclusief de gerelateerde Azure assets/ resources. Dit overzicht stelt gebruikers van het template in staat om te evalueren in hoeverre het template bijdraagt aan de naleving van de BIO per control en overheids-maatregel. Het overzicht (zie bijlage 2) betreft een samenvatting van de detailsysteeminstellingen van het template. Het detailoverzicht van de mapping is opgenomen in bijlage 4. Hier kunnen gebruikers op detailniveau zien welke instellingen gekoppeld zijn aan een BIO control of overheidsmaatregel.
Wij raden gebruikersorganisaties aan de juistheid van deze mapping te controleren, aangezien de inrichting van iedere gebruikersorganisatie kan afwijken en het template van Microsoft onderhevig is aan veranderingen. Voor een actueel overzicht van de gemonitorde instellingen verwijzen naar de Github pagina van het BIO Compliance Initiative Template.

Aandachtspunt 

Wij wijzen gebruikersorganisaties erop dat de compliance statussen (aanbevolen systeeminstellingen) zijn gebaseerd op Microsoft Best Practices (Microsoft Cloud Security Benchmark), die zijn gekoppeld aan BIO-controls en overheidsmaatregelen. We benadrukken dat per control of overheidsmaatregel mogelijk meer of minder gemonitord wordt dan wordt vereist vanuit de BIO. Wij adviseren gebruikersorganisaties om voor elke relevante BIO-control en overheidsmaatregel tenminste het volgende na te gaan:

- BBN-niveau bepalen: Identificeer het toepasselijke BBN-niveau. Dit is afhankelijk van de data en informatiesystemen die op het Azure-platform worden gebruikt.
- Beoordeling van systeemtechnische elementen: Controleer of de Microsoft Best Practices en bijbehorende monitoring toereikend zijn voor zowel de BIO-naleving als interne beleidsvereisten.
- Regelmatige evaluatie van de mapping: Herzie periodiek de mapping (koppeling tussen BIO-controls/overheidsmaatregelen en gemonitorde systeeminstellingen), aangezien het BIO Compliance Initiative Template continu wordt bijgewerkt en deze hierdoor kan wijzigen.

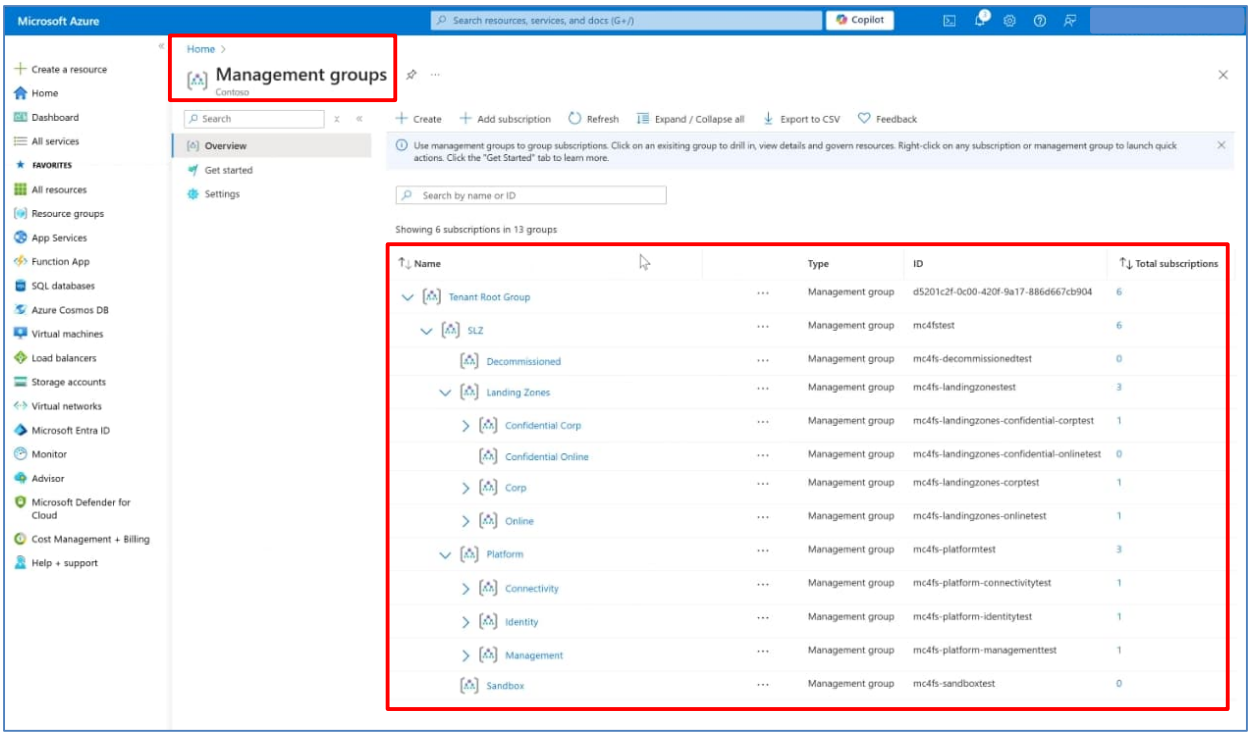
5.3 Fase C: Review monitoring en randvoorwaarden BIO Compliance Initiative Template

In fase C hebben wij de werking en randvoorwaarden van het BIO Compliance Initiative Template onderzocht. Hierin hebben wij drie systeeminstellingen geselecteerd en onderzocht of monitoring in de praktijk effectief werkt. Ook hebben wij de randvoorwaarden voor het effectief gebruiken van template in dit hoofdstuk beschreven. Wij wijzen gebruikersorganisaties erop dat als onderdeel van dit onderzoek slechts drie systeeminstellingen zijn gevalideerd. Wij raden gebruikersorganisaties aan zelf te valideren of de voor hen relevante systeeminstellingen technisch gemonitord worden door het template op het moment dat deze instelling aangezet wordt.

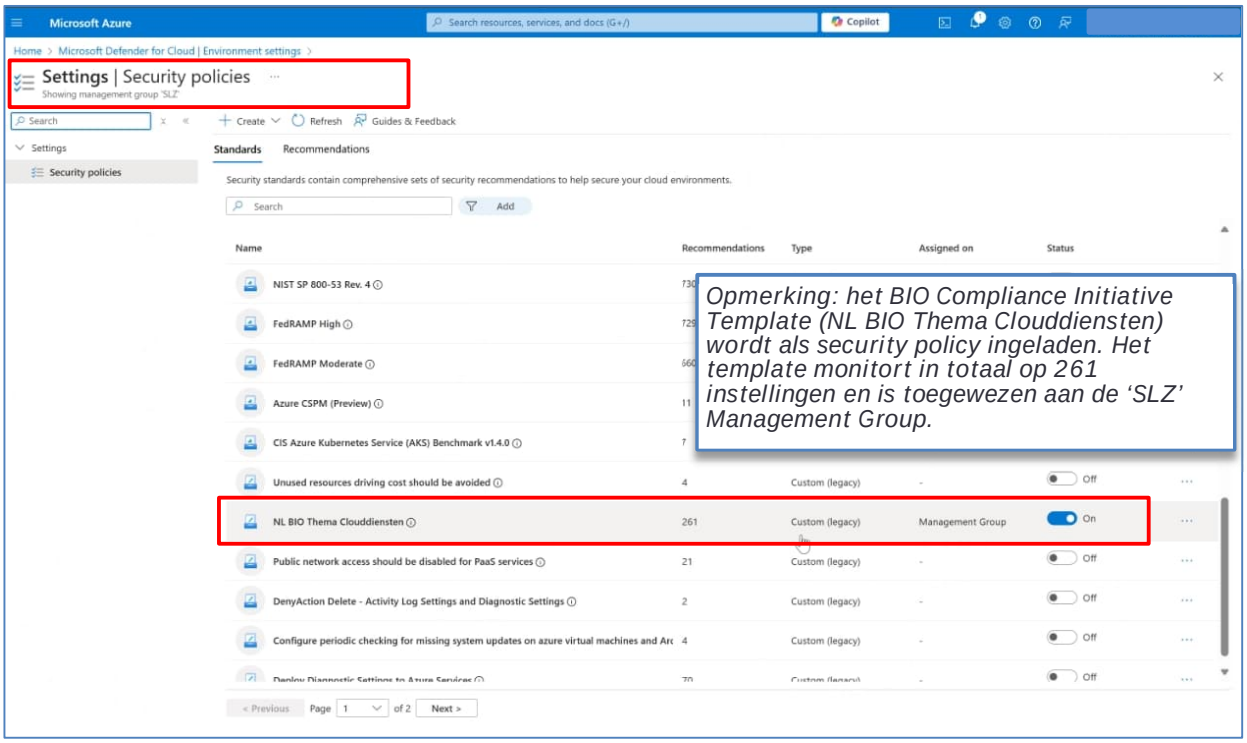
5.3.1 Werking van het BIO Compliance Initiative Template

5.3.1.1 Azure Tenant inrichting

Voorafgaand aan onze validatie heeft Microsoft een Tenant opgezet, bestaande uit een “Sovereign Landing Zone” (SLZ). In sectie 5.1.3 is een toelichting op de inhoud van de SLZ opgenomen. Bij het gebruik van de SLZ worden systeeminstellingen conform het BIO Compliance Initiative Template ingericht en is het template standaard ingeladen in Azure Security Policies. Hierdoor is het niet benodigd het template van Github te downloaden. Het template is door Microsoft geplaatst op de Tenant Root Group. Dit zorgt ervoor dat monitoring door het template actief is voor de gehele tenant, waaronder onderliggende Management Groups en Subscripties. De hiernavolgende afbeeldingen (4 & 5) laten de tenant, inrichting en deployment van het template zien.



Afbeelding 4: Schermprint overzicht Management Groups binnen Tenant



Afbeelding 5: Schermprint Azure Security Policies – BIO Compliance Initiative Template actief

5.3.1.2 Validatiewerkzaamheden

Om de werking van het BIO Compliance Initiative Template te onderzoeken hebben wij drie systeeminstellingen geselecteerd. Deze systeeminstellingen zijn, in afstemming met SLM en Microsoft, risico gebaseerd geselecteerd, waarbij rekening is gehouden met de (toekomstige) relevantie voor clouddiensten binnen overheidsinstellingen.

Tabel 4 (volgende pagina) geeft een overzicht van de systeeminstellingen en onze onderzoeksresultaten weer. Wij hebben voor de drie geselecteerde systeeminstellingen de werking van monitoring gevalideerd. Wij verwijzen naar sectie 8 "Bijlage 3: Validatieresultaten face C" voor de vastleggingen van onze werkzaamheden. Deze werkzaamheden zijn door ons op woensdag 28 augustus 2024 op locatie bij Microsoft uitgevoerd in een SLZ Azure-omgeving (versie 2.3.3 van het template).

Voor elke systeeminstelling hebben wij de volgende werkzaamheden uitgevoerd:

1) De compliant status van de systeeminstelling beoordeeld zoals weergegeven in de monitoring van het template (groen = compliant, rood = niet compliant).
2) Geëvalueerd of de systeeminstelling correct is geconfigureerd volgens de monitoring. Met andere woorden hebben wij gecontroleerd of het template de juiste waarde aangeeft.
3) Indien de systeeminstelling configureerbaar is, hebben wij deze aangepast om de compliant status te wijzigen (compliant/niet compliant). Vervolgens hebben we beoordeeld of de compliant status overeenkomstig werd aangepast in het template.

Tabel 4: Validatiestappen inclusief resultaten voor drie geselecteerde systeeminstellingen binnen het BIO Compliance Initiative Template.

Nr.	Systeem-instelling zoals opgenomen in het template[6]	Toelichting monitoring door BIO Compliance Initiative Template	BIO Control	Validatie resultaten (zie sectie 8 bijlage 3 voor onze vastleggingen)	Conclusie
1	Virtual machines and virtual machine scale sets should have encryption at host enabled	Het template controleert of voor aanwezige Virtuele Machines (VM's) en Virtuele Machine Scale Sets "encryption at host" is ingeschakeld.	10.1.1 10.1.1.2 10.1.2 18.1.5 18.1.5.1	Gevalideerd dat: 1) Het template de compliant status laat zien conform de geconfigureerde systeeminstellingen (juiste waarde). 2) Indien de systeeminstelling wordt gewijzigd de status van het template wijzigt en overeenkomstig is met de wijziging (compliant status laat de juiste waarde zien).	✓ Geen afwijkingen geconstateerd.
2	Role-Based Access Control (RBAC) should be used on Kubernetes Services	Het template controleert of voor aanwezige Kubernetes Services RBAC is ingeschakeld.	6.1.1 9.1.2 9.1.2.1 9.4.1.2	Gevalideerd dat: 1) Het template de compliant status laat zien conform de geconfigureerde systeeminstellingen (juiste waarde). 2) De systeeminstellingen niet configureerbaar zijn. Als onderdeel van het SLZ is het enkel mogelijk voor de gebruiker om RBAC ingeschakeld te hebben voor Kubernetes Services.	✓ Geen afwijkingen geconstateerd.

6 Voor een overzicht van systeeminstellingen (inclusief de drie gevalideerde systeeminstellingen) verwijzen wij naar de Github pagina.

Nr.	Systeem-instelling zoals opgenomen in het template[6]	Toelichting monitoring door BIO Compliance Initiative Template	BIO Control	Validatie resultaten (zie sectie 8 bijlage 3 voor onze vastleggingen)	Conclusie
3	Azure Defender for Key Vault should be enabled	Het template controleert of Azure Defender voor Azure Key Vault is ingeschakeld.	12.2.1 12.2.1.3 12.2.1.5 12.4.1 12.6.1 12.6.1.1	Gevalideerd dat: 1) Het template de compliant status laat zien conform de geconfigureerde systeeminstellingen (juiste waarde). 2) Indien de systeeminstelling wordt gewijzigd de status van het template wijzigt en overeenkomstig is met de wijziging (compliant status laat de juiste waarde zien).	✓ Geen afwijkingen geconstateerd.

5.3.2 Randvoorwaarden bij implementatie BIO Compliance Initiative Template

In fase C hebben wij tevens onderzoek uitgevoerd naar de randvoorwaarden voor gebruikersorganisaties bij de implementatie van het BIO Compliance Initiative Template.

Aandachtspunt 

In fase C hebben wij tevens onderzoek uitgevoerd naar de randvoorwaarden voor gebruikersorganisaties bij de implementatie van het BIO Compliance Initiative Template. Het is hierom van belang dat gebruikersorganisaties alvorens implementatie van het template bewust zijn van onderstaande randvoorwaarden.

Wij onderkennen hierin de volgende onderdelen die in deze paragraaf zijn beschreven:
- Inschakeling van logging (op meldingen en wijzigingen template).
- Periodieke controle op logging of automatische alarmering.
- Templatewijzigingen middels het formele change proces.
- Autorisatiebeheer en functiescheiding.

5.3.2.1 Logging & Controle

Een belangrijk aspect bij het gebruik van het template betreft de inrichting van logging. Hierbij wordt onderscheid gemaakt tussen enerzijds de logging van meldingen (compliant/niet compliant) en anderzijds de logging van wijzigingen aan het template. Dit laatste betreft bijvoorbeeld het filteren van monitoring op systeeminstellingen of resources.

Logging op meldingen

Om voor gebruikersorganisaties en externe auditors vast te stellen of systeeminstellingen gedurende het jaar BIO-compliant zijn geconfigureerd, en de status “compliant” behouden is, is het van belang dat logging wordt ingeschakeld op de status van systeeminstellingen. Dit wordt niet standaard afgedwongen bij de implementatie van het template. Het is de verantwoordelijkheid van de gebruikersorganisatie om deze logging in te schakelen. In Azure kan dit door het inschakelen van Compliance Over Time Workbook. Dit is standaard beschikbaar in Azure en zorgt ervoor dat een automatisch export van de status van instellingen gegeneerd wordt. Om deze logging beschikbaar te maken dient de gebruikersorganisaties deze exports beschikbaar te maken in een log analyse tooling (Zoals Log Analytics). Dit is een aanvullende configuratie binnen Azure. Het inschakelen van logging is noodzakelijk om een audit trail te waarborgen en daarmee de naleving van de BIO gedurende het jaar te bepalen.

Logging op wijzigingen

Naast logging van de status van systeeminstellingen is het van belang om ook logging van wijzigingen aan het template in te schakelen. Hiermee wordt gewaarborgd dat ongeautoriseerde of onwenselijke wijzigingen aan het template herleidbaar is. Het template biedt gebruikersorganisaties namelijk de mogelijkheid om monitoring op diverse manieren aan te passen. Hierbij kan gedacht worden aan:

- het wijzigen van de te monitoren systeeminstellingen;
- het aanpassen van de te monitoren resources of assets;
- het wijzigen van het niveau van monitoring (bijvoorbeeld op management group niveau of subscriptieniveau).

Het activeren van logging, in combinatie met periodieke controles of automatische alarmering (zie onderstaande sectie), kan onwenselijke wijzigingen aan het template voorkomen. Dit is van belang om te voorkomen dat systeeminstellingen voor de gebruikersorganisatie niet langer BIO-compliant zijn geconfigureerd.

Periodieke controle op logging of automatische alarmering

Wij adviseren gebruikersorganisaties om een (periodieke) controle in te richten voor de tijdige opvolging van meldingen die door het template gegenereerd worden (wijzigingen in compliant statussen). Wijzigingen in Azure kunnen ertoe leiden dat systeeminstellingen niet langer compliant zijn met het BIO Compliance Initiative Template. Het is daarom van belang dat de gebruikersorganisatie een verantwoordelijke functionaris aanwijst voor de monitoring van systeeminstellingen. Dit kan worden gerealiseerd door een periodieke controle in te richten, waarbij een verantwoordelijke 1) beoordeelt in hoeverre instellingen compliant zijn geconfigureerd en 2) een controle uitvoert op de logging om tussentijdse niet-compliant systeeminstellingen vast te stellen. Een andere mogelijkheid is om automatische alarmering in te zetten. Binnen Azure is het configureren van automatische alarmering mogelijk via Workflow Automation in Microsoft Defender for Cloud.

Change Proces

Voor het gecontroleerd doorvoeren van wijzigingen aan het template adviseren wij wijzigingen te laten verlopen via de door de gebruikersorganisatie geformaliseerde wijzigingsbeheerprocedure (change proces). Binnen deze procedure is het van belang dat autorisatie plaatsvindt, om ongeautoriseerde wijzigingen van het template te voorkomen. Ook dienen doorgevoerde wijzigingen voldoende getest te worden.

5.3.2.2 Autorisatiebeheer

Naast logging en het gecontroleerd doorvoeren van wijzigingen is het voor gebruikersorganisaties van belang maatregelen te treffen bij de inrichting van autorisaties binnen Azure bij het inzetten van het BIO Compliance Initiative Template. Allereerst dient een gebruikersorganisatie te evalueren op welk niveau het template actief wordt gesteld. Zoals beschreven in Sectie 5.1.1, kunnen gebruikers-organisaties het template op twee manieren implementeren:

- Op management group niveau.
- Op subscriptieniveau.

Op het moment dat het template op management group niveau wordt ingezet, wordt het template actief voor alle onderliggende managementgroepen en subscripties. Indien het template op subscriptieniveau wordt ingezet, wordt de monitoring alleen actief voor de betreffende subscriptie en de onderliggende resources/assets. Afhankelijk op welk niveau het template actief is kunnen bepaalde gebruikers wijzigingen doorvoeren. Op management group niveau betreft dit de “root-user”. Op subscriptieniveau betreft dit de Subscription Owner. Wij bevelen gebruikersorganisaties aan na te gaan in hoeverre het wenselijk is dat functionarissen met een van beide profielen, ofwel root-user/subscriptie owner, de bevoegdheid heeft tot het beheer van het template. Het risico bestaat dat gebruikers met owner-rechten ongeautoriseerde wijzigingen aanbrengen doordat zij zowel configuraties als wijzigingen aan het template kunnen doorvoeren, waardoor mogelijk systeeminstellingen niet meer worden gemonitord.

Functiescheiding tussen IT en templatebeheerders

Om ongeautoriseerde wijzigingen aan het template te voorkomen, adviseren wij om functiescheiding toe te passen tussen gebruikers die verantwoordelijk zijn voor het configureren van systeeminstellingen en de tenantinfrastructuur, en gebruikers die verantwoordelijk zijn voor het monitoren en beheren van het template. Op deze manier wordt voorkomen dat ontwikkelaars of IT-beheerders ongeautoriseerde wijzigingen aan systeeminstellingen doorvoeren zonder dat deze wijzigingen worden gedetecteerd door het template.

6 Bijlage 1: Overzicht van de Cloud gerelateerde BIO controls en overheidsmaatregelen

In deze bijlage is een overzicht opgenomen van BIO-controls en overheidsmaatregelen die toezien op een de technische inrichting van cloudcomponenten met betrekking tot IaaS/PaaS, evenals de BIO-controls en overheidsmaatregelen die worden gemonitord door het BIO Compliance Initiative Template. Voor de totstandkoming van dit overzicht hebben wij per BIO-control en overheidsmaatregel beoordeeld in hoeverre deze een technisch component bevatten dat binnen een IaaS- en PaaS-inrichting gemonitord kan worden, en of er monitoring binnen het template aanwezig is. Het overzicht biedt de gebruikersorganisatie inzicht in de reikwijdte van het template en maakt duidelijk welke controls en overheidsmaatregelen geen deel uitmaken van het template, maar wel relevant zijn bij het gebruik van een cloudoplossing. Het is belangrijk op te merken dat een vermelding van monitoring (“Ja ✓”) niet impliceert dat alle aspecten rondom de betreffende BIO-control gemonitord worden. Voor een samenvatting van de monitoring per BIO control en overheidsmaatregel verwijzen wij naar bijlage 2 tabel 6. Zie tabel 5 hieronder voor het volledige overzicht.

Tabel 5: Detailoverzicht BIO Controls en overheidsmaatregelen met technisch IaaS/PaaS element (Groen = Overheidsmaatregel)

BIO Hoofdstuk	BIO Control en overheids-maatregel (Nr.)	Technische inrichting IaaS/PaaS element binnen control	Monitoring van systeeminstellingen aanwezig in template volgens Microsoft	Toelichting/ verwijzing indien monitoring niet actief is
6. Organiseren van informatiebeveiliging	6.1.1	Ja	Ja ✓	
9. Toegangs-beveiliging	9.1.2	Ja	Ja ✓	
	9.1.2.1	Ja	Ja ✓	
	9.4.1.2	Ja	Ja ✓	
	9.4.2.1	Ja	Nee ×	BIO Overheidsmaat-regel 9.4.2.1 ziet toe op MFA voor vertrouwde zones. Het classificeren van een vertrouwde zone is afhankelijk van de architectuur van de klantomgeving. Deze inrichting vindt middels Azure EntraID plaats.

BIO Hoofdstuk	BIO Control en overheids-maatregel (Nr.)	Technische inrichting IaaS/PaaS element binnen control	Monitoring van systeeminstellingen aanwezig in template volgens Microsoft	Toelichting/ verwijzing indien monitoring niet actief is
				Hiervoor dient separate monitoring door de gebruikers-organisatie ingericht te worden.
	9.4.3	Ja	Ja ✓	
	9.4.3.1	Ja	Ja ✓	
	9.4.3.3	Ja	Ja ✓	
	9.4.3.4	Ja	Ja ✓	
	9.4.3.5	Ja	Ja ✓	
	9.4.5	Ja	Nee ×	Monitoring op toegangsbeveiliging voor toegang tot Infrastructure as Code (of gerelateerde repositories) is geen onderdeel van het template. Ten aanzien van Azure broncode dienen gebruikersorganisaties de relevante Assurance-verklaringen te raadplegen.
10. Cryptografie	10.1.1	Ja	Ja ✓	
	10.1.1.1	Ja	Ja ✓	
	10.1.1.2	Ja	Ja ✓	
	10.1.2	Ja	Ja ✓	
	10.1.2.1	Ja	Ja ✓	
11. Fysieke beveiliging en beveiliging van de omgeving	11.1.1	Ja	Nee ×	Hoofdstuk 11 bevat BIO controls en overheids-maatregelen die toezien op fysieke
	11.1.1.1	Ja	Nee ×	
	11.1.2	Ja	Nee ×	
	11.1.2.1	Ja	Nee ×	
	11. 1.3	Ja	Nee ×	

BIO Hoofdstuk	BIO Control en overheids-maatregel (Nr.)	Technische inrichting IaaS/PaaS element binnen control	Monitoring van systeeminstellingen aanwezig in template volgens Microsoft	Toelichting/ verwijzing indien monitoring niet actief is
	11.1.3.1	Ja	Nee ×	maatregelen en zodoende geen onderdeel zijn van de monitoring van het template. Voor de verantwoordelijk-heden en geïmplementeerde maatregelen van Microsoft ten aanzien van deze controls en overheids-maatregelen verwijzen wij naar het eerder uitgevoerde onderzoek “Onderzoek BIO Compliant gebruik Microsoft” welke gepubliceerd is op de website van SLM Rijk.
	11.1.4	Ja	Nee ×	
	11.1.4.1	Ja	Nee ×	
	11.1.4.2	Ja	Nee ×	
	11.1.5	Ja	Nee ×	
	11.1.6	Ja	Nee ×	
	11.2.1	Ja	Nee ×	
	11.2.2	Ja	Nee ×	
	11.2.3	Ja	Nee ×	
	11.2.4	Ja	Nee ×	
	11.2.5	Ja	Nee ×	
	11.2.6	Ja	Nee ×	
	11.2.7	Ja	Nee ×	
	11.2.8	Ja	Nee ×	
	11.2.9	Ja	Nee ×	
	11.2.9.1	Ja	Nee ×	
	11.2.9.2	Ja	Nee ×	
	11.2.9.3	Ja	Nee ×	
	11.2.9.4	Ja	Nee ×	
	11.2.9.5	Ja	Nee ×	
12. Beveiliging bedrijfsvoering	12.1.3	Ja	Nee ×	Nog geen monitoring voor aanwezig.
	12.1.4	Ja	Nee ×	BIO Control ziet toe op scheiding tussen ontwikkel-, test- en productie-omgevingen. Deze inrichting is afhankelijk van de architectuur van de gebruikers-organisatie.

BIO Hoofdstuk	BIO Control en overheids-maatregel (Nr.)	Technische inrichting IaaS/PaaS element binnen control	Monitoring van systeeminstellingen aanwezig in template volgens Microsoft	Toelichting/ verwijzing indien monitoring niet actief is
				Hierom dient separate monitoring door de gebruikers-organisatie ingericht te worden.
	12.2.1	Ja	Ja ✓	
	12.2.1.3	Ja	Ja ✓	
	12.2.1.5	Ja	Ja ✓	
	12.3.1	Ja	Ja ✓	
	12.3.1.3	Ja	Ja ✓	
	12.3.1.4	Ja	Ja ✓	
	12.4.1	Ja	Ja ✓	
	12.4.1.3	Ja	Nee ×	BIO Overheidsmaat-regel ziet toe op de aanwezigheid van SOC/SIEM monitoring. Hier dient separate monitoring door de gebruikers-organisatie ingericht te worden.
	12.4.3	Ja	Nee ×	Monitoring op de logging van activiteiten van beheerders is binnen het template actief (12.4.1). Er vindt geen monitoring plaats op de beoordeling van deze activiteiten.

BIO Hoofdstuk	BIO Control en overheids-maatregel (Nr.)	Technische inrichting IaaS/PaaS element binnen control	Monitoring van systeeminstellingen aanwezig in template volgens Microsoft	Toelichting/ verwijzing indien monitoring niet actief is
	12.4.4	Ja	Nee ×	Geen monitoring voor actief in het template. Configuratie is standaard actief binnen Azure.
	12.6.1	Ja	Ja ✓	
	12.6.1.1	Ja	Ja ✓	
	12.6.2	Ja	Ja ✓	
	12.6.2.1	Ja	Ja ✓	
13. Communicatie-beveiliging	13.1.1	Ja	Ja ✓	
	13.1.2	Ja	Ja ✓	
	13.1.2.1	Ja	Nee ×	BIO Overheids-maatregel ziet toe op de aanwezig-heid van detectie-voorzieningen. Hier dient separate monitoring door de gebruikers-organisatie ingericht te worden.
	13.1.2.4	Ja	Ja ✓	
17. Informatiebeveiligings-aspecten van bedrijfscontinuïteits-beheer	17.2.1	Ja	Ja ✓	
18. Naleving	18.1.1	Ja	Ja ✓	
	18.1.5	Ja	Ja ✓	
	18.1.5.1	Ja	Ja ✓	

7 Bijlage 2: BIO Compliance Initiative Template - Overzicht gemonitorde BIO controls en overheidsmaatregelen

In deze bijlage is het overzicht opgenomen met daarin een samenvatting van de monitoring van het BIO Compliance Initiative Template. Per BIO control of overheidsmaatregel is de scope van monitoring samengevat. Voor een detailoverzicht van de mapping verwijzen wij naar de bijlage 4 als onderdeel van dit rapport. In deze bijlage is, voor gebruikersorganisaties, in detailniveau inzichtelijk welke instellingen gekoppeld zijn aan een BIO-control of -overheidsmaatregel. Wij adviseren gebruikersorganisaties aan de juistheid van dit overzicht te controleren voor hun specifieke situatie.

Tabel 6: Overzicht van Azure instellingen gemonitord door het BIO Compliance Initiative Template

BIO	Control beschrijving	Instellingen gemonitord door het BIO Compliance Initiative Template
6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging: Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Het template monitort op diverse autorisatie- en authenticatie-instellingen, waaronder: • Maximaal 3 subscription owners per subscription. • Verwijdering van geblokkeerde- en gast-accounts. • Multi Factor Authentication (MFA) voor Admin accounts. • Inschakeling van Microsoft Entra-only authentication voor Databaseservers en Azure Synapse workspaces. • Inschakeling van RBAC voor Kubernetes. • “Audit usage” voor customised RBAC-rollen. • Aanwezigheid Microsoft Entra administrator voor PostgreSQL servers.
9.1.2	Toegang tot netwerken en netwerkdiensten: Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Het template monitort diverse autorisatie- en authenticatie-instellingen, waaronder: • Maximaal 3 subscription owners per subscription. • Minimaal 1 subscription owner. • Verwijdering van geblokkeerde- en gast-accounts. • MFA voor Admin accounts. • Inschakeling van Microsoft Entra-only authentication voor Databaseservers en Azure Synapse workspaces. • Inschakeling van RBAC voor Kubernetes en “Audit usage” voor gecustomiseerde RBAC-rollen. • Uitschakeling van lokale authenticatiemethoden voor Azure Machine Learning en Cognitive Services.

BIO	Control beschrijving	Instellingen gemonitord door het BIO Compliance Initiative Template
		• Inschakeling van Managed Identity voor App service apps en Azure Function apps. • Toegang van accounts zonder wachtwoord voor VM's (Linux). • Gedeelde sleuteltoegang voor Storage Accounts (niet toegestaan). • Toegang tot SQL-server door een Azure AD Admin. • Inschakeling Azure AD voor VPN-gateway (Point-to-site users). Het template monitort daarnaast specifiek op: • Migratie naar nieuwe Azure Resource Manager resources voor VM's en Storage Accounts. • Controle op het gebruik van "unmanaged" disks voor Virtuele Machines (VM's).
9.1.2.1	Alleen geauthentiseerde apparatuur kan toegang krijgen tot een vertrouwde zone.	Het template monitort diverse autorisatie- en authenticatie-instellingen, waaronder: • Maximaal 3 subscription owners per subscription. • Minimaal 1 subscription owner. • Verwijdering van geblokkeerde- en gast-accounts. • MFA voor Admin accounts. • Inschakeling van Microsoft Entra-only authentication voor Databaseservers en Azure Synapse workspaces. • Inschakeling van RBAC voor Kubernetes en "Audit usage" voor gecustomiseerde RBAC-rollen. • Uitschakeling van lokale authenticatiemethoden voor Azure Machine Learning en Cognitive Services. • Inschakeling van Managed Identity voor App service apps en Azure Function apps. • Toegang van accounts zonder wachtwoord voor VM's (Linux). • Gedeelde sleuteltoegang voor Storage Accounts (niet toegestaan). • Toegang tot SQL-server door een Azure AD Admin. • Inschakeling Azure AD voor VPN-gateway (Point-to-site users). Het template monitort daarnaast specifiek op: • Migratie naar nieuwe Azure Resource Manager resources voor VM's en Storage Accounts. • Controle op het gebruik van "unmanaged" disks voor VM's.

BIO	Control beschrijving	Instellingen gemonitord door het BIO Compliance Initiative Template
9.4.1.2	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	Het template monitort diverse autorisatie- en authenticatie-instellingen, waaronder: • Maximaal 3 subscription owners per subscription. • Minimaal 1 subscription owner. • Verwijdering van geblokkeerde- en gast-accounts. • MFA voor Admin accounts. • Inschakeling van Microsoft Entra-only authentication voor Databaseservers en Azure Synapse workspaces. • Inschakeling van RBAC voor Kubernetes en “Audit usage” voor gecustomiseerde RBAC-rollen. • Uitschakeling van lokale authenticatiemethoden voor Azure Machine Learning en Cognitive Services. • Inschakeling van Managed Identity voor App service apps en Azure Function apps. • Toegang van accounts zonder wachtwoord voor VM’s (Linux). • Gedeelde sleuteltoegang voor Storage Accounts (niet toegestaan). • Toegang tot SQL-server door een Azure AD Admin. • Inschakeling Azure AD voor VPN-gateway (Point-to-site users). Het template monitort daarnaast specifiek op: • Migratie naar nieuwe Azure Resource Manager resources voor VM’s en Storage Accounts. • Controle op het gebruik van “unmanaged” disks voor VM’s.
9.4.3	Systeem voor wachtwoordbeheer: Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	Het template monitort of “Guest Configuration”-extensie geïnstalleerd is voor VM’s.

BIO	Control beschrijving	Instellingen gemonitord door het BIO Compliance Initiative Template
9.4.3.1	Als er geen gebruik wordt gemaakt van two-factor authenticatie, is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal foutieve inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen, is vastgelegd.	Het template monitort of “Guest Configuration”-extensie geïnstalleerd is voor VM’s.
9.4.3.3	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	Het template monitort of “Guest Configuration”-extensie geïnstalleerd is voor VM’s.
9.4.3.4	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.	Het template monitort of “Guest Configuration”-extensie geïnstalleerd is voor VM’s.
9.4.3.5	Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.	Het template monitort of “Guest Configuration”-extensie geïnstalleerd is voor VM’s.
10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen: Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	Het template monitort op de aanwezigheid van diverse soorten encryptie, waaronder: • Customer Managed Keys encryptie voor Azure Services, Virtuele Machinees, Databases, OS en Storage Accounts. • Disk encryptie en host encryptie voor Azure Services en VM’s. • Dubbele encryptie voor Azure Services en Managed Disks. • Infrastructuur encryptie voor Databaseservers en Managed Disks. • Transparante data encryptie voor Databaseservers. Het template monitort op de inschakeling van Guest attestation-extensie, Secure booting en TPM voor VM’s en logging van queries voor Azure Monitor.

BIO	Control beschrijving	Instellingen gemonitord door het BIO Compliance Initiative Template
10.1.1.1	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	Het template monitort op de aanwezigheid van diverse soorten encryptie, waaronder: • Disk encryptie voor VM's. • Passende Encryptie protocollen, waaronder HTTPS, FTPS, TLS en SSL voor Azure Services, Databaseservers en Kubernetes. • Transparante data encryptie voor Databaseservers. • Encryptie "in transit" voor Azure HDInsight. • Encryptie van Automation account variables. Het template monitort op de inschakeling van "Secure Transfer" voor Storage Accounts en "EncryptAndSign" voor ClusterProtectionLevel.
10.1.1.2	Crypografische toepassingen voldoen aan passende standaarden.	Het template monitort op de aanwezigheid van diverse soorten encryptie, waaronder: • Customer Managed Keys encryptie voor Azure Services, VM's, Databases, OS en Storage Accounts. • Disk encryptie en host encryptie voor Azure Services en VM's. • Dubbele encryptie voor Azure Services en Managed Disks. • Infrastructuur encryptie voor Databaseservers en Managed Disks. • Transparante data encryptie voor Databaseservers. Het template monitort op de inschakeling van Guest attestation-extensie, Secure booting en TPM voor VM's en logging van queries voor Azure Monitor.

BIO	Control beschrijving	Instellingen gemonitord door het BIO Compliance Initiative Template
10.1.2	Sleutelbeheer: Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.	Het template monitort op de aanwezigheid van diverse soorten encryptie, waaronder: • Customer Managed Keys encryptie voor Azure Services, VM's, Databases, OS en Storage Accounts. • Disk encryptie en host encryptie voor Azure Services en VM's. • Dubbele encryptie voor Azure Services en Managed Disks. • Infrastructuur encryptie voor Databaseservers en Managed Disks. • Transparante data encryptie voor Databaseservers. Het template monitort op de inschakeling van Guest attestation-extensie, Secure booting en TPM voor VM's en logging van queries voor Azure Monitor.
10.1.2.1	Ingeval van PKI-overheid certificaten: hanteer de PKI-Overheid-eisen t.a.v. het sleutelbeheer. In overige situaties: hanteer de standaard ISO-11770 voor het beheer van cryptografische sleutels.	Het template monitort op de aanwezigheid van diverse soorten encryptie, waaronder: • Disk encryptie voor VM's. • Passende Encryptie protocollen, waaronder HTTPS, FTPS, TLS en SSL voor Azure Services, Databaseservers en Kubernetes. • Transparante data encryptie voor Databaseservers. • Encryptie "in transit" voor Azure HDInsight. • Encryptie van Automation account variables. Het template monitort op de inschakeling van "Secure Transfer" voor Storage Accounts en "EncryptAndSign" voor ClusterProtectionLevel.

BIO	Control beschrijving	Instellingen gemonitord door het BIO Compliance Initiative Template
12.2.1	Beheersmaatregelen tegen malware: Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	Het template monitort of vulnerability scanning (tooling), waaronder Azure Defender en Defender for Cloud, is ingeschakeld voor VM's, DNS, Azure Services, Containers en Databases. Het template monitort of kwetsbaarheden gemitigeerd zijn voor Containers, VM's en Databases en automatische updates uitgevoerd worden voor VM's. Het template monitort of (security) waarschuwingen gemaild worden naar subscription owners. Het template monitort op specifieke instellingen waaronder: • Veilige versie Kubernetes services. • Veilige http-versie voor Function Apps. • Inschakeling WAF voor Applicatie Gateway en Azure Front Door. • Inschakeling End Point protectie voor Azure Security Center en VM's. • Inschakeling DDOS Protectie. • Uitschakeling van IP Forwarding voor VM's.
12.2.1.3	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.	Het template monitort of vulnerability scanning (tooling), waaronder Azure Defender en Defender for Cloud, is ingeschakeld voor VM's, DNS, Azure Services, Containers en Databases. Het template monitort of kwetsbaarheden gemitigeerd zijn voor Containers, VM's en Databases en automatische updates uitgevoerd worden voor VM's. Het template monitort of (security) waarschuwingen gemaild worden naar subscription owners. Het template monitort op specifieke instellingen waaronder: • Veilige versie Kubernetes services. • Veilige http-versie voor Function Apps. • Inschakeling WAF voor Applicatie Gateway en Azure Front Door.

BIO	Control beschrijving	Instellingen gemonitord door het BIO Compliance Initiative Template
		• Inschakeling End Point protectie voor Azure Security Center en VM's. • Inschakeling DDOS Protectie. • Uitschakeling van IP Forwarding voor VM's.
12.2.1.5	De malware scan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld op mailservers, desktop-computers en bij de toegang tot het netwerk van de organisatie.	Het template monitort of vulnerability scanning (tooling), waaronder Azure Defender en Defender for Cloud, is ingeschakeld voor VM's, DNS, Azure Services, Containers en Databases. Het template monitort of kwetsbaarheden gemitigeerd zijn voor Containers, VM's en Databases en automatische updates uitgevoerd worden voor VM's. Het template monitort of (security) waarschuwingen gemaild worden naar subscription owners. Het template monitort op specifieke instellingen waaronder: • Veilige versie van Kubernetes services. • Veilige http-versie voor Function Apps. • Inschakeling WAF voor Applicatie Gateway en Azure Front Door. • Inschakeling End Point protectie voor Azure Security Center en VM's. • Inschakeling DDOS Protectie. • Uitschakeling van IP Forwarding voor VM's.
12.3.1	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Het template monitort specifiek op de: • Inschakeling van Azure Backup voor VM's. • Inschakeling van disaster recovery voor VM's. • Inschakeling deletion protection voor Key vaults. • Inschakeling soft delete voor Key vaults.

BIO	Control beschrijving	Instellingen gemonitord door het BIO Compliance Initiative Template
12.3.1.3	In het back-upbeleid staan minimaal de volgende eisen: (a) Dataverlies bedraagt maximaal 28 uur. (b) Hersteltijd in geval van incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen.	Het template monitort specifiek op de: • Inschakeling van Azure Backup voor VM's. • Inschakeling van disaster recovery voor VM's. • Inschakeling deletion protection voor Key vaults. • Inschakeling soft delete voor Key vaults.
12.3.1.4	Het back-up proces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.	Het template monitort specifiek op de: • Inschakeling van Geo-redundatbackups voor Azure Database for MariaDB. • Inschakeling van Geo-redundatbackups voor Azure Database for MySQL. • Inschakeling van Geo-redundatbackups voor Azure Database for PostgreSQL.
12.4.1	Gebeurtenissen registreren: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Het template monitort of vulnerability scanning (tooling), waaronder Azure Defender en Defender for Cloud, is ingeschakeld voor VM's, DNS, Azure Services, Containers en Databases. Het template monitort op de aanwezigheid van diverse soorten logging, waaronder: • Resource logs voor Azure Services. • Netwerkverkeer voor VM's. • Log analytics voor VM's en Azure Arc Machines. Het template monitort op specifieke instelligen, waaronder: • Inschakeling automatische toekenning Log analytics agents. • Inschakeling "Guest configuration" en "Dependency Agents" voor VM's. • Inschakeling Auditing voor SQL-servers. • Inschakeling Audit diagnostics. • Inschakeling Network Watcher. • Installatie van Azure Monitor Agent voor VM's en Azure Arc Machines.
12.6.1	Beheer van technische kwetsbaarheden: Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende	Het template monitort of vulnerability scanning (tooling), waaronder Azure Defender en Defender for Cloud, is ingeschakeld voor VM's, DNS, Azure Services, Containers en Databases en, of Endpoint protection is ingeschakeld voor VM's en Azure Security Center.

BIO	Control beschrijving	Instellingen gemonitord door het BIO Compliance Initiative Template
	maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.	Het template monitort of kwetsbaarheden gemitigeerd zijn voor Containers, VM's en Databases en automatische updates uitgevoerd worden voor VM's. Het template monitort op de veiligheid van configuraties voor Kubernetes-clustercontainers, zoals AppArmor profielen, gebruik van toegestane poorten, het niet toekennen van CAP_SYS_ADMIN, AKS, et cetera. Het template monitort of voor App Service apps en Azure Funtion apps: • Veilige versies, ten aanzien van Python/Java/PHP, worden gebruikt. • Uitschakeling van externe debugging. • Juiste configuratie van CORS. • Laatste http-versie wordt gebruikt.
12.6.1.1	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheids-waarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.	Het template monitort of vulnerability scanning (tooling), waaronder Azure Defender en Defender for Cloud, is ingeschakeld voor VM's, DNS, Azure Services, Containers en Databases en of Endpoint protection is ingeschakeld voor VM's en Azure Security Center. Het template monitort of kwetsbaarheden gemitigeerd zijn voor Containers, VM's en Databases en automatische updates uitgevoerd worden voor VM's. Het template monitort of voor App Service apps en Azure Function apps: • Veilige versies, ten aanzien van Python/Java/PHP, worden gebruikt. • Laatste http-versie wordt gebruikt.
12.6.2	Beperkingen voor het installeren van software: Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	Het template monitort op specifieke instellingen, waaronder: • Inschakeling van Azure Defender for Servers. • Inschakeling van adaptive application controls for defining safe applications voor VM's. • Geüpdatete allowlist rules in adpative application control policy.

BIO	Control beschrijving	Instellingen gemonitord door het BIO Compliance Initiative Template
12.6.2.1	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).	Het template monitort op specifieke instellingen, waaronder: • Inschakeling van Azure Defender for servers. • Inschakeling van adaptive application controls for defining safe applications voor VM's. • Geüpdatete allowlist rules in adpative application control policy.
13.1.1	Beheersmaatregelen voor netwerken: Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Het template monitort of (netwerk)toegang veilig is geconfigureerd, waaronder een controle of: • Private Link is ingeschakeld voor Azure Services, Containers, Disk access resources en Storage Accounts. • Publieke netwerktoegang is uitgeschakeld voor Azure Services, Databaseservers, Containers en Storage Accounts. • Private endpoint is ingeschakeld voor Databaseservers, Azure Machine Learning en Cognitive Services-accounts. • Netwerkpoorten gekoppeld zijn aan Network Security Groups voor VM's en Subnets. • Virtual Network (rules) worden gebruikt voor Azure Services en Storage Accounts. • WAF is ingeschakeld voor Webapps en Application Gateway. • Firewall is ingeschakeld voor Azure Key Vault en Azure Cosmos DB (accounts). • Adaptive network hardening aanbevelingen zijn ingeschakeld voor VM's. • Geautoriseerde IP-ranges zijn gedefinieerd voor Kubernetes-services.
13.1.2	Beveiliging van netwerkdiensten: Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Het template monitort op specifieke instellingen, waaronder: • Inschakeling WAF voor applicatie gateway. • Uitschakeling IP Forwarding voor VM's. • DDOS Protectie. • Inschakeling Azure Web app Firewall voor Webapps. • Beperkte netwerktoegang door Storage Accounts. • Koppeling netwerkpoorten aan Network Security Groups voor VM's.

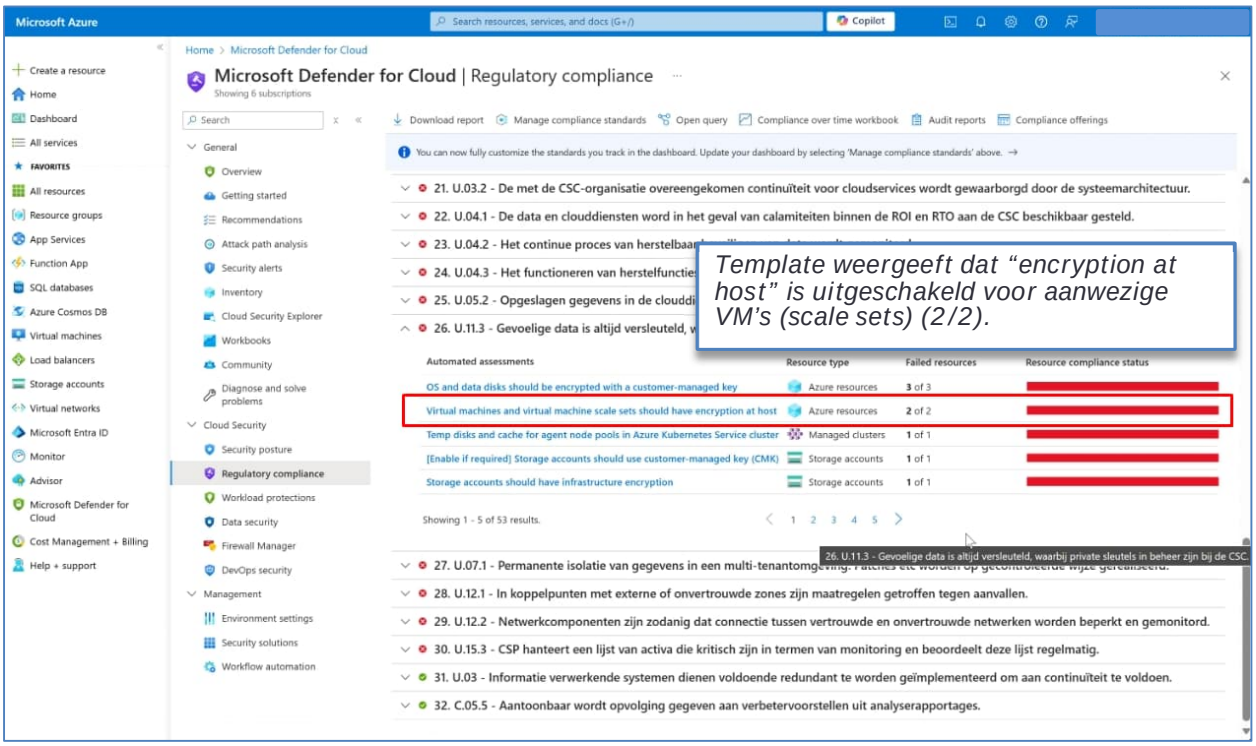
BIO	Control beschrijving	Instellingen gemonitord door het BIO Compliance Initiative Template
13.1.2.4	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en hierop te reageren.	Het template monitort op specifieke instellingen, waaronder: • Inschakeling WAF voor applicatie gateway. • Uitschakeling IP Forwarding voor VM's. • DDOS Protectie. • Inschakeling Azure Web app Firewall voor Webapps. • Beperkte netwerktoegang door Storage Accounts. • Koppeling netwerkpoorten aan Network Security Groups voor VM's.
17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten: Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Het template monitort specifiek op de: • Inschakeling van Geo-redundatbackups voor Azure Database for MariaDB. • Inschakeling van Geo-redundatbackups voor Azure Database for MySQL. • Inschakeling van Geo-redundatbackups voor Azure Database for PostgreSQL. • Inschakeling van Azure Backup voor VM's. • Inschakeling van disaster recovery voor VM's.
18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen: Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen behoren voor elk informatie-systeem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.	Het template monitort of enkel toegestane locaties gebruikt worden (resources actief op toegestane datacenter locaties).
18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen: Cryptografische beheersmaat-regelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	Het template monitort op de aanwezigheid van diverse soorten encryptie, waaronder: • Customer Managed Keys encryptie voor Azure Services, VM's, Databases, OS en Storage Accounts. • Disk encryptie en host encryptie voor Azure Services en VM's. • Dubbele encryptie voor Azure Services en Managed Disks. • Infrastructuur encryptie voor Databaseservers en Managed Disks. • Transparante data encryptie voor Databaseservers. Het template monitort op de inschakeling van Guest attestation-extensie, Secure booting en TPM voor VM's en logging van queries voor Azure Monitor.

BIO	Control beschrijving	Instellingen gemonitord door het BIO Compliance Initiative Template
18.1.5.1	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de “pas toe of leg uit”-lijst van het Forum.	Het template monitort op de aanwezigheid van diverse soorten encryptie, waaronder: • Customer Managed Keys encryptie voor Azure Services, VM’s, Databases, OS en Storage Accounts. • Disk encryptie en host encryptie voor Azure Services en VM’s. • Dubbele encryptie voor Azure Services en Managed Disks. • Infrastructuur encryptie voor Databaseservers en Managed Disks. • Transparante data encryptie voor Databaseservers. Het template monitort op de inschakeling van Guest attestation-extensie, Secure booting en TPM voor VM’s en logging van queries voor Azure Monitor.

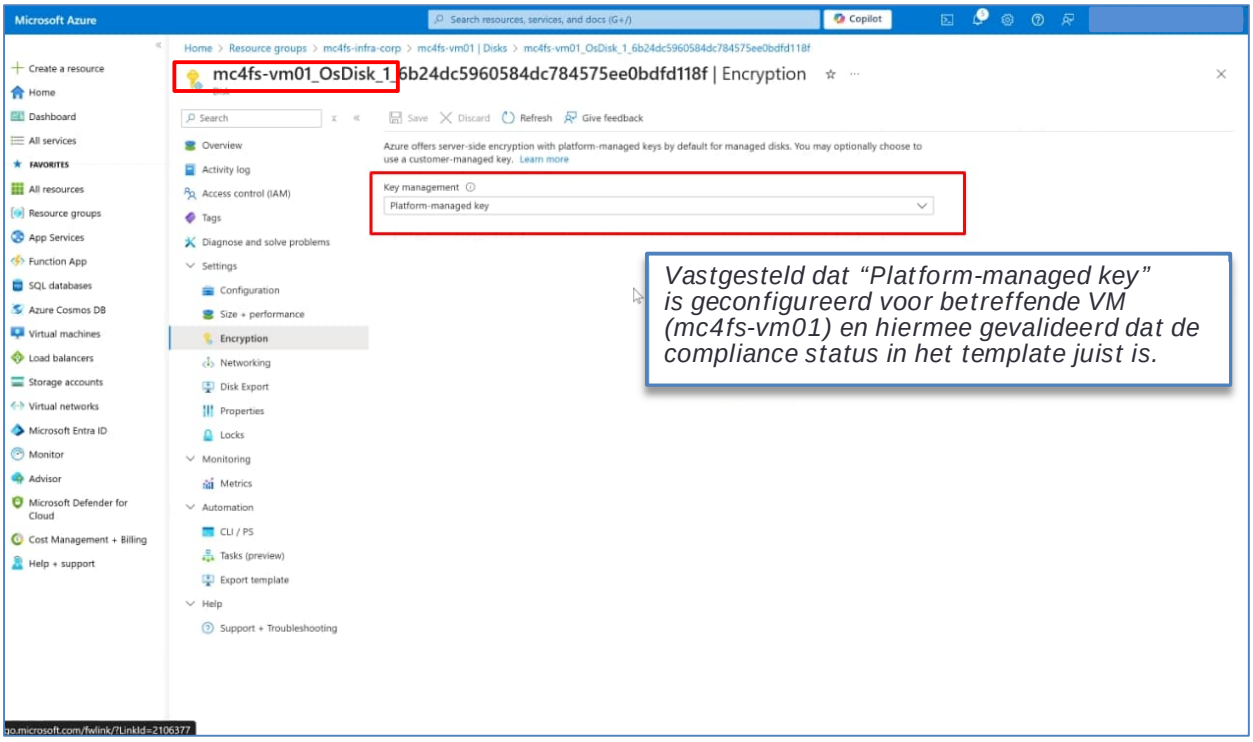
8 Bijlage 3: Validatieresultaten fase C

In deze bijlage zijn de details van de validatie resultaten uit fase C opgenomen. Als onderdeel van onze werkzaamheden hebben wij drie systeeminstellingen uit het BIO Compliance Initiative Template geselecteerd en de werking van monitoring gevalideerd. Deze validatie heeft plaatsgevonden in een SLZ Azure-omgeving. De vastlegging van onze werkzaamheden maakt voor de gebruikersorganisatie inzichtelijk op welke wijze systeeminstellingen binnen het template gevalideerd kunnen worden op de juiste monitoring. Onderstaand onze vastleggingen per systeeminstelling.

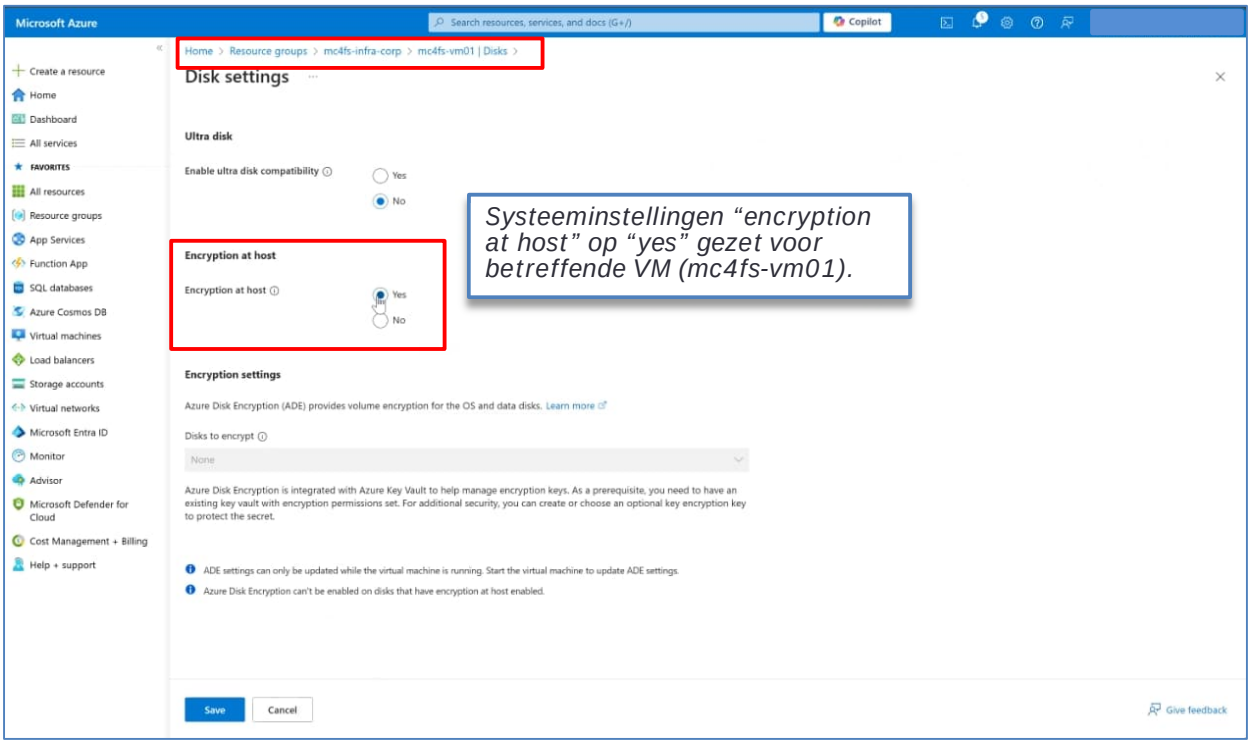
8.1 Virtual machines and virtual machine scale sets should have encryption at host enabled.



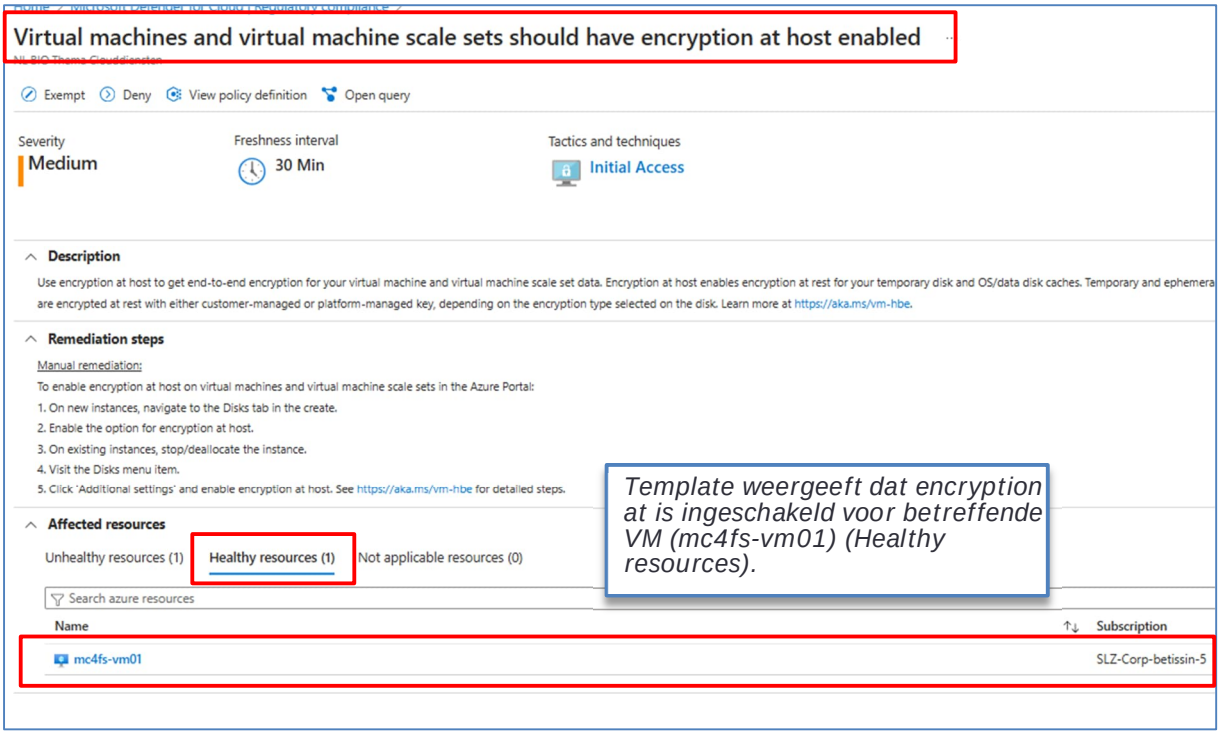
Afbeelding 6: Validatiewerkzaamheden “Virtual machines and virtual machine scale sets should have encryption at host enabled” (1)



Afbeelding 7: Validatiewerkzaamheden “Virtual machines and virtual machine scale sets should have encryption at host enabled” (2)

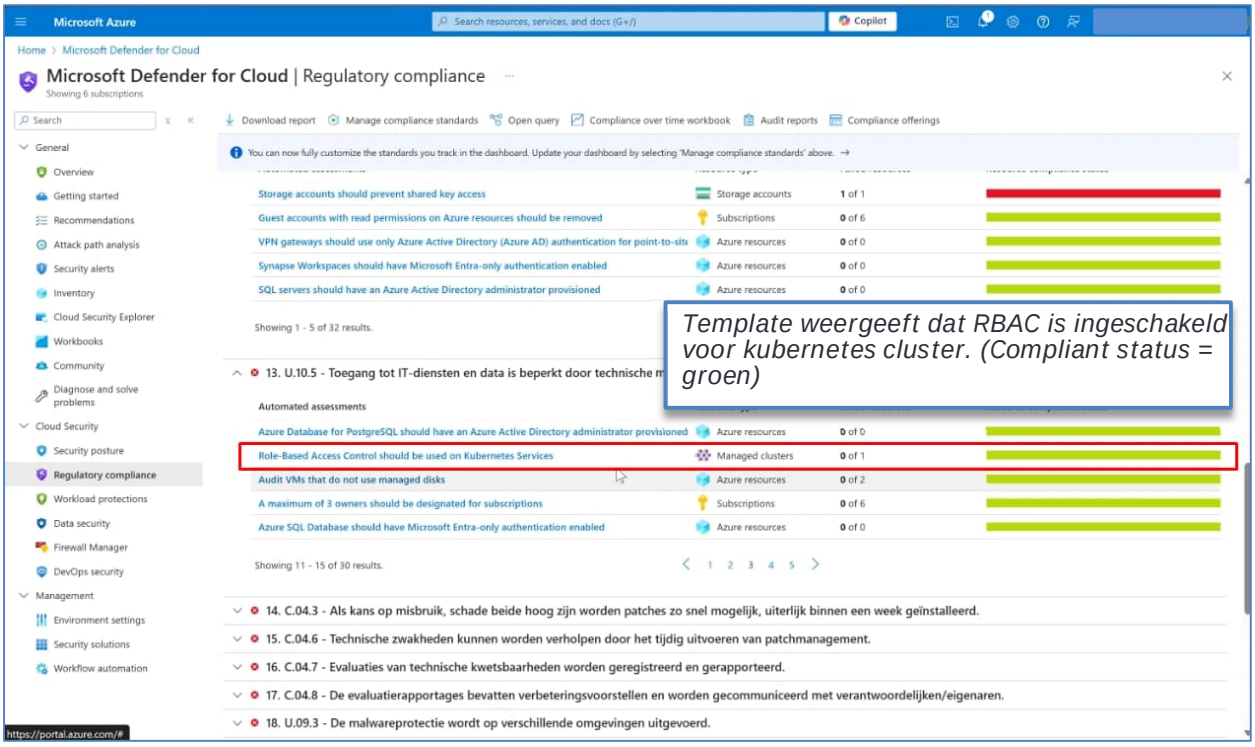


Afbeelding 8: Validatiewerkzaamheden “Virtual machines and virtual machine scale sets should have encryption at host enabled” (3)

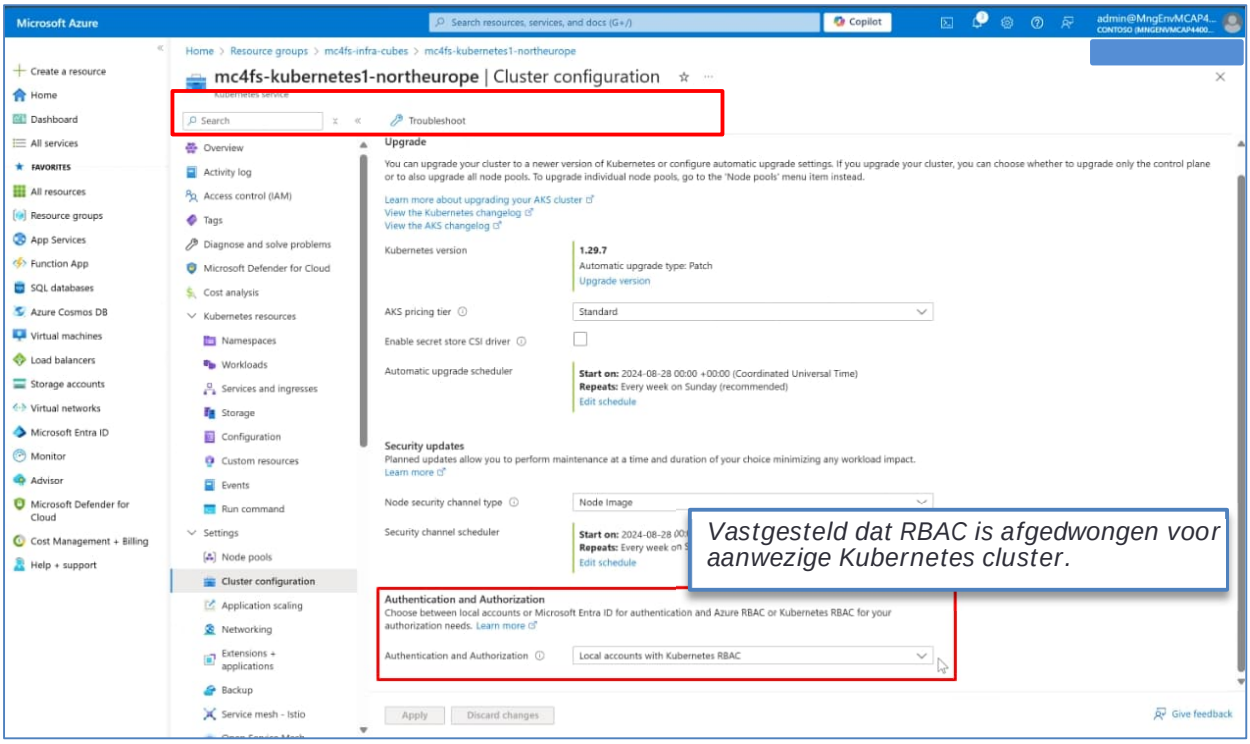


Afbeelding 9: Validatiewerkzaamheden "Virtual machines and virtual machine scale sets should have encryption at host enabled" (4)

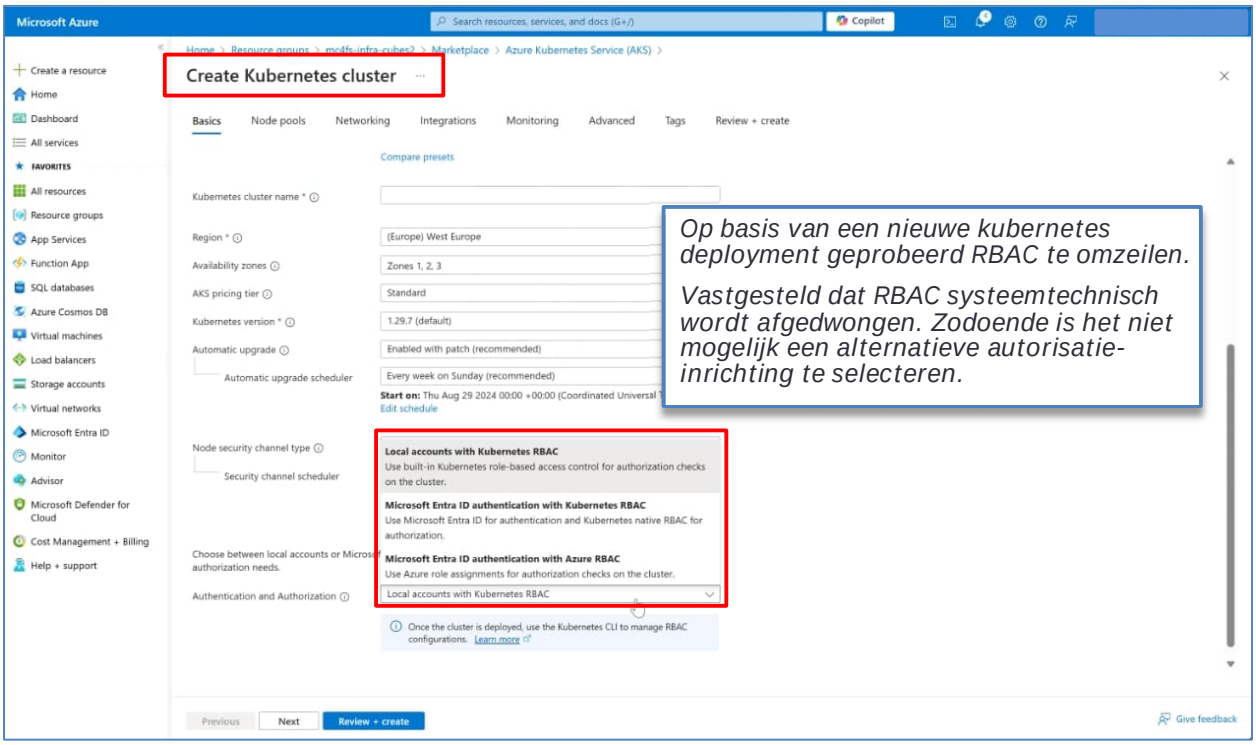
8.2 Role-Based Access Control (RBAC) should be used on Kubernetes Services



Afbeelding 10: Validatiewerkzaamheden "Role-Based Access Control (RBAC) should be used on Kubernetes Services" (1)

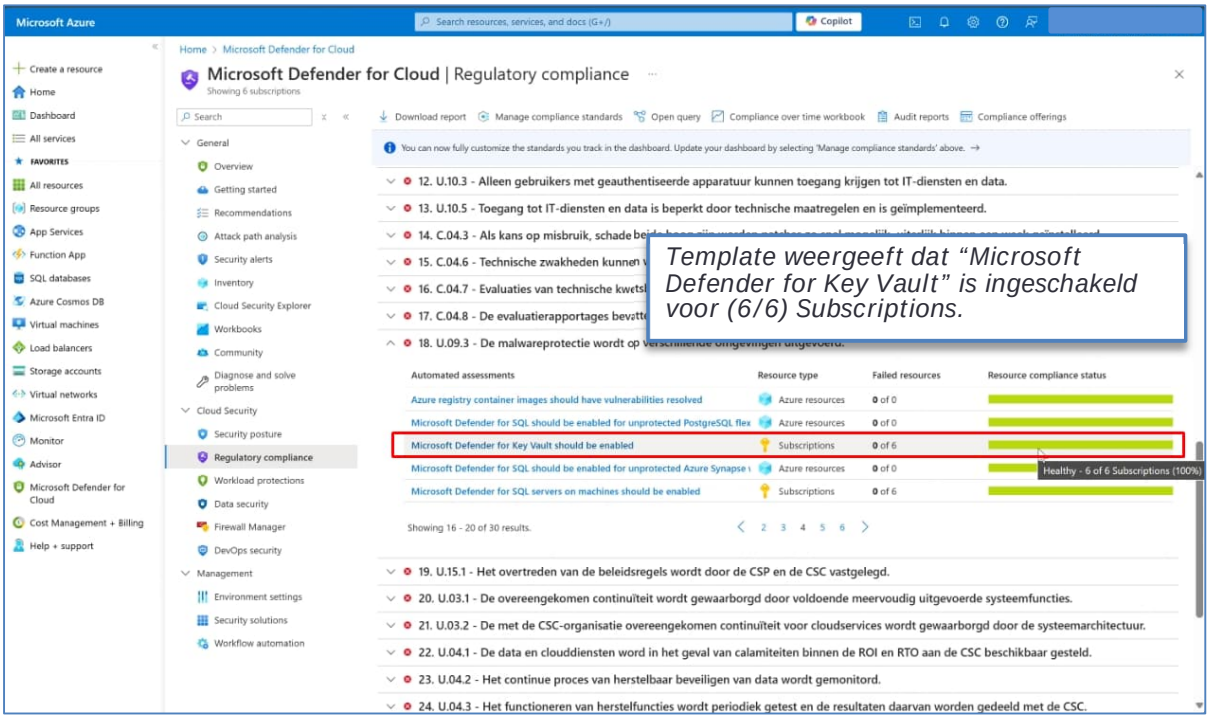


Afbeelding 11: Validatiewerkzaamheden "Role-Based Access Control (RBAC) should be used on Kubernetes Services" (2)

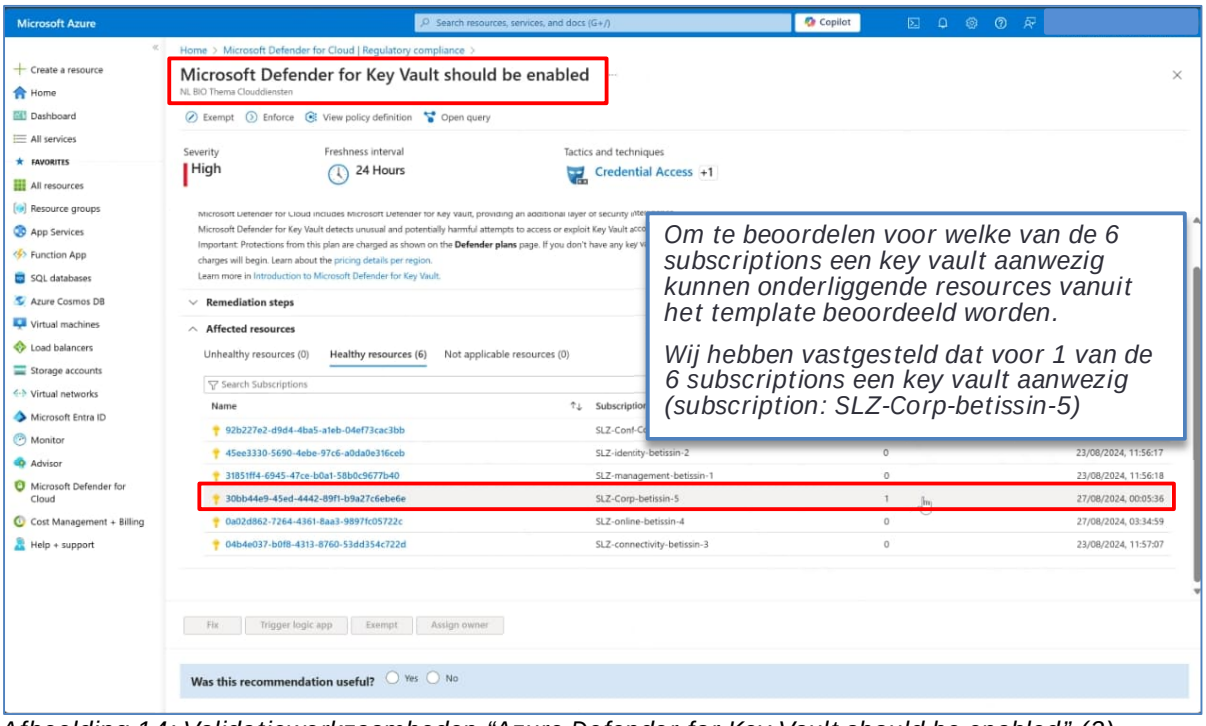


Afbeelding 12: Validatiewerkzaamheden "Role-Based Access Control (RBAC) should be used on Kubernetes Services" (3)

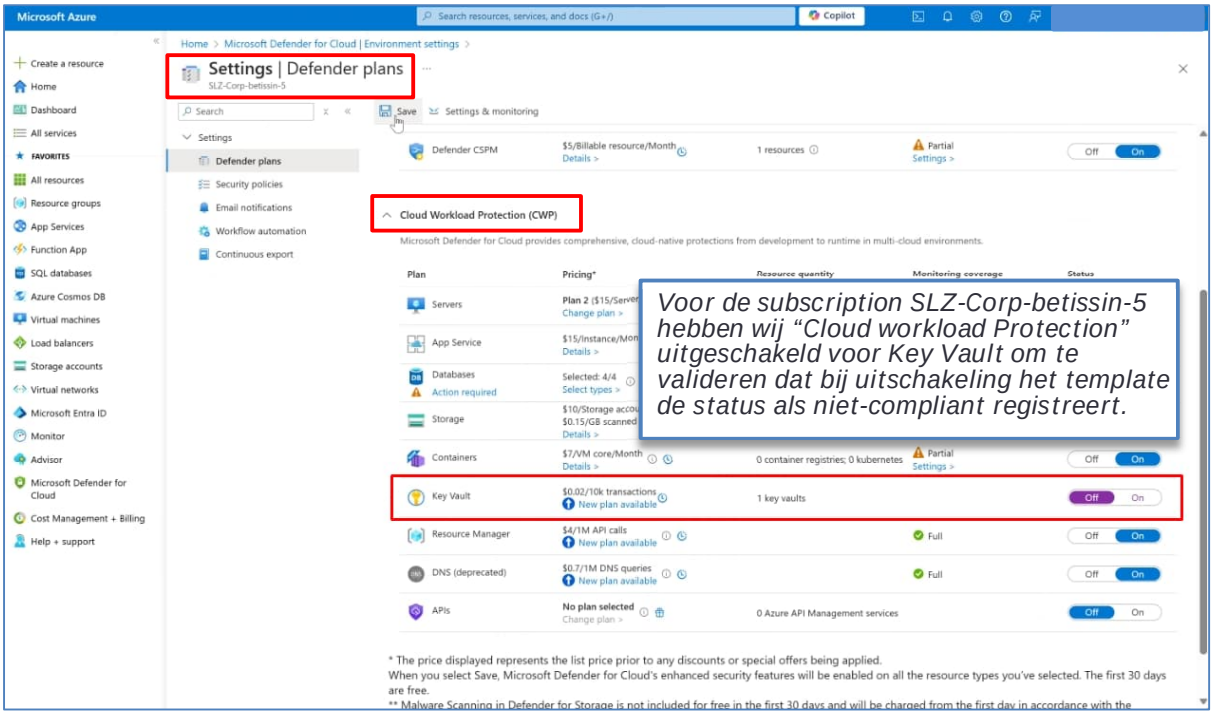
8.3 Azure Defender for Key Vault should be enabled



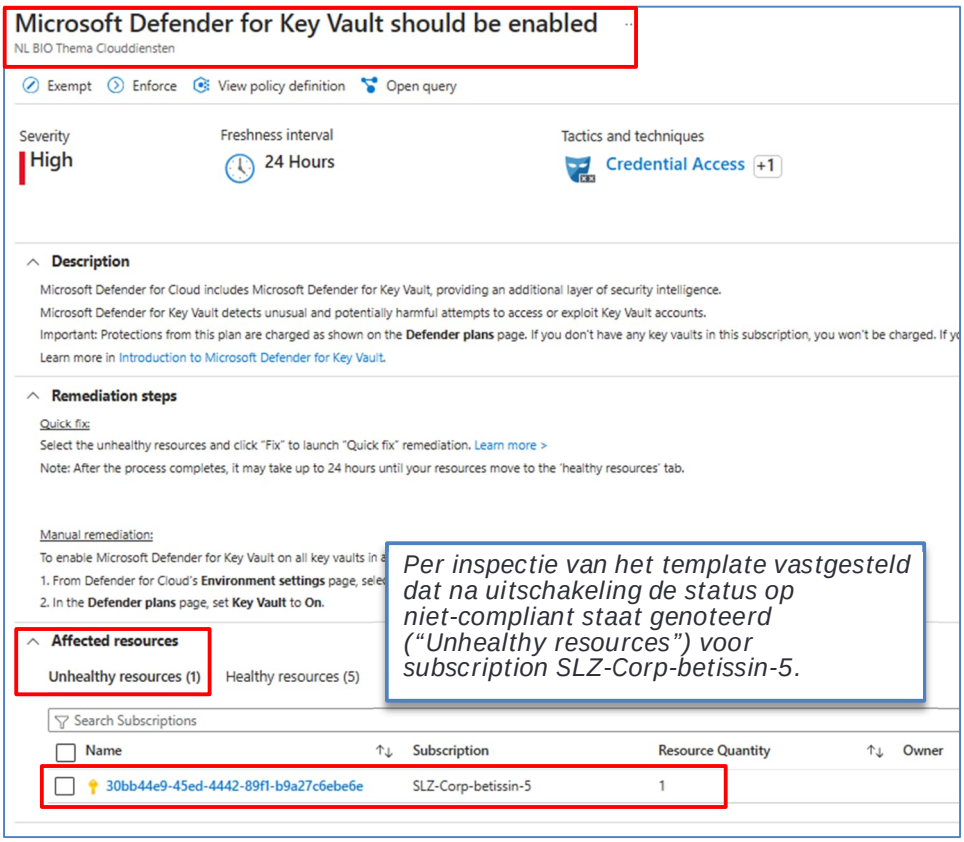
Afbeelding 13: Validatiewerkzaamheden “Azure Defender for Key Vault should be enabled” (1)



Afbeelding 14: Validatiewerkzaamheden “Azure Defender for Key Vault should be enabled” (2)



Afbeelding 15: Validatiewerkzaamheden "Azure Defender for Key Vault should be enabled" (3)



Afbeelding 16: Validatiewerkzaamheden "Azure Defender for Key Vault should be enabled" (4)

9 Bijlage 4: Mapping BIO controls en overheidsmaatregelen met detail templatesettings

In deze bijlage is een overzicht opgenomen waarin per templatesetting de gerelateerde BIO-control of overheidsmaatregel wordt weergegeven. Dit overzicht biedt de gebruikersorganisatie inzicht in de wijze waarop onze mapping van gemonitorde BIO-controls en overheidsmaatregelen tot stand is gekomen. Voor een samenvatting van de monitoring verwijzen wij naar sectie 8, bijlage 3. Het overzicht bevat de templatesettings afkomstig uit versie 2.2.3 van het BIO Compliance Initiative Template. Wij adviseren gebruikersorganisaties de juistheid van dit overzicht te controleren in het kader van hun specifieke situatie.

Tabel 7: Overzicht van templatesettings per BIO control of overheidsmaatregel

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
6.1.1	Azure SQL Database should have Microsoft Entra-only authentication enabled
6.1.1	Azure SQL Database should have Microsoft Entra-only authentication enabled during creation
6.1.1	Azure SQL Managed Instance should have Microsoft Entra-only authentication enabled
6.1.1	Azure SQL Managed Instances should have Microsoft Entra-only authentication enabled during creation
6.1.1	Synapse Workspaces should have Microsoft Entra-only authentication enabled
6.1.1	Synapse Workspaces should use only Microsoft Entra identities for authentication during workspace creation
6.1.1	A Microsoft Entra administrator should be provisioned for PostgreSQL servers
6.1.1	Role-Based Access Control (RBAC) should be used on Kubernetes Services
6.1.1	Audit usage of custom RBAC roles
6.1.1	A maximum of 3 owners should be designated for your subscription
6.1.1	Blocked accounts with owner permissions on Azure resources should be removed
6.1.1	Guest accounts with write permissions on Azure resources should be removed
6.1.1	Blocked accounts with owner permissions on Azure resources should be removed
6.1.1	Blocked accounts with read and write permissions on Azure resources should be removed
6.1.1	Guest accounts with read permissions on Azure resources should be removed
6.1.1	Guest accounts with owner permissions on Azure resources should be removed
6.1.1	Accounts with read permissions on Azure resources should be MFA enabled

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
6.1.1	Accounts with owner permissions on Azure resources should be MFA enabled
6.1.1	Accounts with write permissions on Azure resources should be MFA enabled
9.1.2	App Service apps should use managed identity
9.1.2	Function apps should use managed identity
9.1.2	Azure Machine Learning Computes should have local authentication methods disabled
9.1.2	Accounts with owner permissions on Azure resources should be MFA enabled
9.1.2	Accounts with read permissions on Azure resources should be MFA enabled
9.1.2	Accounts with write permissions on Azure resources should be MFA enabled
9.1.2	A maximum of 3 owners should be designated for your subscription
9.1.2	Audit usage of custom RBAC roles
9.1.2	Guest accounts with owner permissions on Azure resources should be removed
9.1.2	Guest accounts with read permissions on Azure resources should be removed
9.1.2	Guest accounts with write permissions on Azure resources should be removed
9.1.2	Blocked accounts with owner permissions on Azure resources should be removed
9.1.2	Blocked accounts with read and write permissions on Azure resources should be removed
9.1.2	Synapse Workspaces should use only Microsoft Entra identities for authentication during workspace creation
9.1.2	Synapse Workspaces should have Microsoft Entra-only authentication enabled
9.1.2	Cognitive Services accounts should have local authentication methods disabled
9.1.2	Role-Based Access Control (RBAC) should be used on Kubernetes Services
9.1.2	Audit Linux machines that allow remote connections from accounts without passwords
9.1.2	Audit Linux machines that have accounts without passwords
9.1.2	A Microsoft Entra administrator should be provisioned for PostgreSQL servers
9.1.2	Service Fabric clusters should only use Azure Active Directory for client authentication
9.1.2	Azure SQL Managed Instance should have Microsoft Entra-only authentication enabled
9.1.2	Azure SQL Managed Instances should have Microsoft Entra-only authentication enabled during creation
9.1.2	Azure SQL Database should have Microsoft Entra-only authentication enabled

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
9.1.2	Azure SQL Database should have Microsoft Entra-only authentication enabled during creation
9.1.2	An Azure Active Directory administrator should be provisioned for SQL servers
9.1.2	Storage accounts should prevent shared key access
9.1.2	Storage accounts should be migrated to new Azure Resource Manager resources
9.1.2	There should be more than one owner assigned to your subscription
9.1.2	Audit VMs that do not use managed disks
9.1.2	Virtual machines should be migrated to new Azure Resource Manager resources
9.1.2	VPN gateways should use only Azure Active Directory (Azure AD) authentication for point-to-site users
9.1.2.1	Azure SQL Database should have Microsoft Entra-only authentication enabled
9.1.2.1	Azure SQL Database should have Microsoft Entra-only authentication enabled during creation
9.1.2.1	Azure SQL Managed Instance should have Microsoft Entra-only authentication enabled
9.1.2.1	Azure SQL Managed Instances should have Microsoft Entra-only authentication enabled during creation
9.1.2.1	Synapse Workspaces should have Microsoft Entra-only authentication enabled
9.1.2.1	Synapse Workspaces should use only Microsoft Entra identities for authentication during workspace creation
9.1.2.1	A maximum of 3 owners should be designated for your subscription
9.1.2.1	Accounts with owner permissions on Azure resources should be MFA enabled
9.1.2.1	Accounts with read permissions on Azure resources should be MFA enabled
9.1.2.1	Accounts with write permissions on Azure resources should be MFA enabled
9.1.2.1	An Azure Active Directory administrator should be provisioned for SQL servers
9.1.2.1	App Service apps should use managed identity
9.1.2.1	Audit Linux machines that allow remote connections from accounts without passwords
9.1.2.1	Audit Linux machines that have accounts without passwords
9.1.2.1	Audit usage of custom RBAC roles
9.1.2.1	Audit VMs that do not use managed disks
9.1.2.1	Azure Machine Learning Computes should have local authentication methods disabled
9.1.2.1	Blocked accounts with owner permissions on Azure resources should be removed

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
9.1.2.1	Blocked accounts with read and write permissions on Azure resources should be removed
9.1.2.1	Cognitive Services accounts should have local authentication methods disabled
9.1.2.1	Function apps should use managed identity
9.1.2.1	Guest accounts with owner permissions on Azure resources should be removed
9.1.2.1	Guest accounts with read permissions on Azure resources should be removed
9.1.2.1	Guest accounts with write permissions on Azure resources should be removed
9.1.2.1	Role-Based Access Control (RBAC) should be used on Kubernetes Services
9.1.2.1	Service Fabric clusters should only use Azure Active Directory for client authentication
9.1.2.1	Storage accounts should be migrated to new Azure Resource Manager resources
9.1.2.1	Storage accounts should prevent shared key access
9.1.2.1	There should be more than one owner assigned to your subscription
9.1.2.1	Virtual machines should be migrated to new Azure Resource Manager resources
9.1.2.1	VPN gateways should use only Azure Active Directory (Azure AD) authentication for point-to-site users
9.4.1.2	Azure SQL Database should have Microsoft Entra-only authentication enabled
9.4.1.2	Azure SQL Database should have Microsoft Entra-only authentication enabled during creation
9.4.1.2	Azure SQL Managed Instance should have Microsoft Entra-only authentication enabled
9.4.1.2	Azure SQL Managed Instances should have Microsoft Entra-only authentication enabled during creation
9.4.1.2	Synapse Workspaces should have Microsoft Entra-only authentication enabled
9.4.1.2	Synapse Workspaces should use only Microsoft Entra identities for authentication during workspace creation
9.4.1.2	A Microsoft Entra administrator should be provisioned for PostgreSQL servers
9.4.1.2	A maximum of 3 owners should be designated for your subscription
9.4.1.2	Accounts with owner permissions on Azure resources should be MFA enabled
9.4.1.2	Accounts with read permissions on Azure resources should be MFA enabled
9.4.1.2	Accounts with write permissions on Azure resources should be MFA enabled
9.4.1.2	An Azure Active Directory administrator should be provisioned for SQL servers
9.4.1.2	App Service apps should use managed identity

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
9.4.1.2	Audit Linux machines that allow remote connections from accounts without passwords
9.4.1.2	Audit Linux machines that have accounts without passwords
9.4.1.2	Audit usage of custom RBAC roles
9.4.1.2	Audit VMs that do not use managed disks
9.4.1.2	Azure Machine Learning Computes should have local authentication methods disabled
9.4.1.2	Blocked accounts with owner permissions on Azure resources should be removed
9.4.1.2	Blocked accounts with read and write permissions on Azure resources should be removed
9.4.1.2	Cognitive Services accounts should have local authentication methods disabled
9.4.1.2	Function apps should use managed identity
9.4.1.2	Guest accounts with owner permissions on Azure resources should be removed
9.4.1.2	Guest accounts with read permissions on Azure resources should be removed
9.4.1.2	Guest accounts with write permissions on Azure resources should be removed
9.4.1.2	Role-Based Access Control (RBAC) should be used on Kubernetes Services
9.4.1.2	Service Fabric clusters should only use Azure Active Directory for client authentication
9.4.1.2	Storage accounts should be migrated to new Azure Resource Manager resources
9.4.1.2	Storage accounts should prevent shared key access
9.4.1.2	There should be more than one owner assigned to your subscription
9.4.1.2	Virtual machines should be migrated to new Azure Resource Manager resources
9.4.1.2	VPN gateways should use only Azure Active Directory (Azure AD) authentication for point-to-site users
9.4.3	Guest Configuration extension should be installed on your machines
9.4.3.1	Guest Configuration extension should be installed on your machines
9.4.3.3	Guest Configuration extension should be installed on your machines
9.4.3.4	Guest Configuration extension should be installed on your machines
9.4.3.5	Guest Configuration extension should be installed on your machines
10.1.1	Azure HDInsight clusters should use encryption at host to encrypt data at rest
10.1.1	Virtual machines and virtual machine scale sets should have encryption at host enabled

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
10.1.1	[Preview]: Azure Recovery Services vaults should use customer-managed keys for encrypting backup data
10.1.1	[Preview]: IoT Hub device provisioning service data should be encrypted using customer-managed keys (CMK)
10.1.1	Azure API for FHIR should use a customer-managed key to encrypt data at rest
10.1.1	Azure Automation accounts should use customer-managed keys to encrypt data at rest
10.1.1	Azure Batch account should use customer-managed keys to encrypt data
10.1.1	Azure Container Instance container group should use customer-managed key for encryption
10.1.1	Azure Cosmos DB accounts should use customer-managed keys to encrypt data at rest
10.1.1	Azure Data Box jobs should use a customer-managed key to encrypt the device unlock password
10.1.1	Azure Data Explorer encryption at rest should use a customer-managed key
10.1.1	Azure data factories should be encrypted with a customer-managed key
10.1.1	Azure HDInsight clusters should use customer-managed keys to encrypt data at rest
10.1.1	Azure Machine Learning workspaces should be encrypted with a customer-managed key
10.1.1	Azure Monitor Logs clusters should be encrypted with customer-managed key
10.1.1	Azure Stream Analytics jobs should use customer-managed keys to encrypt data
10.1.1	Azure Synapse workspaces should use customer-managed keys to encrypt data at rest
10.1.1	Bot Service should be encrypted with a customer-managed key
10.1.1	Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys
10.1.1	Cognitive Services accounts should enable data encryption with a customer-managed key
10.1.1	Container registries should be encrypted with a customer-managed key
10.1.1	Event Hub namespaces should use a customer-managed key for encryption
10.1.1	HPC Cache accounts should use customer-managed key for encryption
10.1.1	Logic Apps Integration Service Environment should be encrypted with customer-managed keys
10.1.1	MySQL servers should use customer-managed keys to encrypt data at rest
10.1.1	OS and data disks should be encrypted with a customer-managed key
10.1.1	PostgreSQL servers should use customer-managed keys to encrypt data at rest
10.1.1	Service Bus Premium namespaces should use a customer-managed key for encryption

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
10.1.1	SQL servers should use customer-managed keys to encrypt data at rest
10.1.1	Storage account encryption scopes should use customer-managed keys to encrypt data at rest
10.1.1	Storage accounts should use customer-managed key for encryption
10.1.1	Azure Batch pools should have disk encryption enabled
10.1.1	Disk encryption should be enabled on Azure Data Explorer
10.1.1	Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host
10.1.1	Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources
10.1.1	Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.
10.1.1	Linux virtual machines should enable Azure Disk Encryption or EncryptionAtHost.
10.1.1	Azure Data Box jobs should enable double encryption for data at rest on the device
10.1.1	Azure Edge Hardware Center devices should have double encryption support enabled
10.1.1	Azure Monitor Logs clusters should be created with infrastructure-encryption enabled (double encryption)
10.1.1	Double encryption should be enabled on Azure Data Explorer
10.1.1	Managed disks should be double encrypted with both platform-managed and customer-managed keys
10.1.1	Infrastructure encryption should be enabled for Azure Database for MySQL servers
10.1.1	Infrastructure encryption should be enabled for Azure Database for PostgreSQL servers
10.1.1	Storage accounts should have infrastructure encryption
10.1.1	Transparent Data Encryption on SQL databases should be enabled
10.1.1	[Preview]: Guest Attestation extension should be installed on supported Linux virtual machines
10.1.1	[Preview]: Guest Attestation extension should be installed on supported Windows virtual machines
10.1.1	[Preview]: Guest Attestation extension should be installed on supported Linux virtual machines scale sets
10.1.1	[Preview]: Guest Attestation extension should be installed on supported Windows virtual machines scale sets
10.1.1	Saved-queries in Azure Monitor should be saved in customer storage account for logs encryption
10.1.1	[Preview]: Secure Boot should be enabled on supported Windows virtual machines
10.1.1	[Preview]: vTPM should be enabled on supported virtual machines
10.1.1	SQL managed instances should use customer-managed keys to encrypt data at rest

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
10.1.1.1	Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign
10.1.1.1	Automation account variables should be encrypted
10.1.1.1	Azure HDInsight clusters should use encryption in transit to encrypt communication between Azure HDInsight cluster nodes
10.1.1.1	Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources
10.1.1.1	Audit Windows machines that do not store passwords using reversible encryption
10.1.1.1	App Service apps should only be accessible over HTTPS
10.1.1.1	App Service apps should require FTPS only
10.1.1.1	App Service apps should use the latest TLS version
10.1.1.1	Enforce SSL connection should be enabled for MySQL database servers
10.1.1.1	Enforce SSL connection should be enabled for PostgreSQL database servers
10.1.1.1	Function apps should only be accessible over HTTPS
10.1.1.1	Function apps should require FTPS only
10.1.1.1	Function apps should use the latest TLS version
10.1.1.1	Kubernetes clusters should be accessible only over HTTPS
10.1.1.1	Only secure connections to your Azure Cache for Redis should be enabled
10.1.1.1	Windows web servers should be configured to use secure communication protocols
10.1.1.1	Transparent Data Encryption on SQL databases should be enabled
10.1.1.1	Secure transfer to storage accounts should be enabled
10.1.1.2	Azure HDInsight clusters should use encryption at host to encrypt data at rest
10.1.1.2	Virtual machines and virtual machine scale sets should have encryption at host enabled
10.1.1.2	[Preview]: Azure Recovery Services vaults should use customer-managed keys for encrypting backup data
10.1.1.2	[Preview]: IoT Hub device provisioning service data should be encrypted using customer-managed keys (CMK)
10.1.1.2	Azure API for FHIR should use a customer-managed key to encrypt data at rest
10.1.1.2	Azure Automation accounts should use customer-managed keys to encrypt data at rest
10.1.1.2	Azure Batch account should use customer-managed keys to encrypt data
10.1.1.2	Azure Container Instance container group should use customer-managed key for encryption

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
10.1.1.2	Azure Cosmos DB accounts should use customer-managed keys to encrypt data at rest
10.1.1.2	Azure Data Box jobs should use a customer-managed key to encrypt the device unlock password
10.1.1.2	Azure Data Explorer encryption at rest should use a customer-managed key
10.1.1.2	Azure data factories should be encrypted with a customer-managed key
10.1.1.2	Azure HDInsight clusters should use customer-managed keys to encrypt data at rest
10.1.1.2	Azure Machine Learning workspaces should be encrypted with a customer-managed key
10.1.1.2	Azure Monitor Logs clusters should be encrypted with customer-managed key
10.1.1.2	Azure Stream Analytics jobs should use customer-managed keys to encrypt data
10.1.1.2	Azure Synapse workspaces should use customer-managed keys to encrypt data at rest
10.1.1.2	Bot Service should be encrypted with a customer-managed key
10.1.1.2	Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys
10.1.1.2	Cognitive Services accounts should enable data encryption with a customer-managed key
10.1.1.2	Container registries should be encrypted with a customer-managed key
10.1.1.2	Event Hub namespaces should use a customer-managed key for encryption
10.1.1.2	HPC Cache accounts should use customer-managed key for encryption
10.1.1.2	Logic Apps Integration Service Environment should be encrypted with customer-managed keys
10.1.1.2	MySQL servers should use customer-managed keys to encrypt data at rest
10.1.1.2	OS and data disks should be encrypted with a customer-managed key
10.1.1.2	PostgreSQL servers should use customer-managed keys to encrypt data at rest
10.1.1.2	Service Bus Premium namespaces should use a customer-managed key for encryption
10.1.1.2	SQL servers should use customer-managed keys to encrypt data at rest
10.1.1.2	Storage account encryption scopes should use customer-managed keys to encrypt data at rest
10.1.1.2	Storage accounts should use customer-managed key for encryption
10.1.1.2	Azure Batch pools should have disk encryption enabled
10.1.1.2	Disk encryption should be enabled on Azure Data Explorer
10.1.1.2	Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
10.1.1.2	Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources
10.1.1.2	Azure Data Box jobs should enable double encryption for data at rest on the device
10.1.1.2	Azure Edge Hardware Center devices should have double encryption support enabled
10.1.1.2	Azure Monitor Logs clusters should be created with infrastructure-encryption enabled (double encryption)
10.1.1.2	Double encryption should be enabled on Azure Data Explorer
10.1.1.2	Managed disks should be double encrypted with both platform-managed and customer-managed keys
10.1.1.2	Infrastructure encryption should be enabled for Azure Database for MySQL servers
10.1.1.2	Infrastructure encryption should be enabled for Azure Database for PostgreSQL servers
10.1.1.2	Storage accounts should have infrastructure encryption
10.1.1.2	Transparent Data Encryption on SQL databases should be enabled
10.1.1.2	[Preview]: Guest Attestation extension should be installed on supported Linux virtual machines
10.1.1.2	[Preview]: Guest Attestation extension should be installed on supported Windows virtual machines
10.1.1.2	[Preview]: Guest Attestation extension should be installed on supported Linux virtual machines scale sets
10.1.1.2	[Preview]: Guest Attestation extension should be installed on supported Windows virtual machines scale sets
10.1.1.2	Saved-queries in Azure Monitor should be saved in customer storage account for logs encryption
10.1.1.2	[Preview]: Secure Boot should be enabled on supported Windows virtual machines
10.1.1.2	[Preview]: vTPM should be enabled on supported virtual machines
10.1.1.2	SQL managed instances should use customer-managed keys to encrypt data at rest
10.1.2	Azure HDInsight clusters should use encryption at host to encrypt data at rest
10.1.2	Virtual machines and virtual machine scale sets should have encryption at host enabled
10.1.2	[Preview]: Azure Recovery Services vaults should use customer-managed keys for encrypting backup data
10.1.2	[Preview]: IoT Hub device provisioning service data should be encrypted using customer-managed keys (CMK)
10.1.2	Azure API for FHIR should use a customer-managed key to encrypt data at rest
10.1.2	Azure Automation accounts should use customer-managed keys to encrypt data at rest
10.1.2	Azure Batch account should use customer-managed keys to encrypt data
10.1.2	Azure Container Instance container group should use customer-managed key for encryption

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
10.1.2	Azure Cosmos DB accounts should use customer-managed keys to encrypt data at rest
10.1.2	Azure Data Box jobs should use a customer-managed key to encrypt the device unlock password
10.1.2	Azure Data Explorer encryption at rest should use a customer-managed key
10.1.2	Azure data factories should be encrypted with a customer-managed key
10.1.2	Azure HDInsight clusters should use customer-managed keys to encrypt data at rest
10.1.2	Azure Machine Learning workspaces should be encrypted with a customer-managed key
10.1.2	Azure Monitor Logs clusters should be encrypted with customer-managed key
10.1.2	Azure Stream Analytics jobs should use customer-managed keys to encrypt data
10.1.2	Azure Synapse workspaces should use customer-managed keys to encrypt data at rest
10.1.2	Bot Service should be encrypted with a customer-managed key
10.1.2	Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys
10.1.2	Cognitive Services accounts should enable data encryption with a customer-managed key
10.1.2	Container registries should be encrypted with a customer-managed key
10.1.2	Event Hub namespaces should use a customer-managed key for encryption
10.1.2	HPC Cache accounts should use customer-managed key for encryption
10.1.2	Logic Apps Integration Service Environment should be encrypted with customer-managed keys
10.1.2	MySQL servers should use customer-managed keys to encrypt data at rest
10.1.2	OS and data disks should be encrypted with a customer-managed key
10.1.2	PostgreSQL servers should use customer-managed keys to encrypt data at rest
10.1.2	Service Bus Premium namespaces should use a customer-managed key for encryption
10.1.2	SQL servers should use customer-managed keys to encrypt data at rest
10.1.2	Storage account encryption scopes should use customer-managed keys to encrypt data at rest
10.1.2	Storage accounts should use customer-managed key for encryption
10.1.2	Azure Batch pools should have disk encryption enabled
10.1.2	Disk encryption should be enabled on Azure Data Explorer
10.1.2	Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
10.1.2	Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources
10.1.2	Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.
10.1.2	Linux virtual machines should enable Azure Disk Encryption or EncryptionAtHost.
10.1.2	Azure Data Box jobs should enable double encryption for data at rest on the device
10.1.2	Azure Edge Hardware Center devices should have double encryption support enabled
10.1.2	Azure Monitor Logs clusters should be created with infrastructure-encryption enabled (double encryption)
10.1.2	Double encryption should be enabled on Azure Data Explorer
10.1.2	Managed disks should be double encrypted with both platform-managed and customer-managed keys
10.1.2	Infrastructure encryption should be enabled for Azure Database for MySQL servers
10.1.2	Infrastructure encryption should be enabled for Azure Database for PostgreSQL servers
10.1.2	Storage accounts should have infrastructure encryption
10.1.2	Transparent Data Encryption on SQL databases should be enabled
10.1.2	[Preview]: Guest Attestation extension should be installed on supported Linux virtual machines
10.1.2	[Preview]: Guest Attestation extension should be installed on supported Windows virtual machines
10.1.2	[Preview]: Guest Attestation extension should be installed on supported Linux virtual machines scale sets
10.1.2	[Preview]: Guest Attestation extension should be installed on supported Windows virtual machines scale sets
10.1.2	Saved-queries in Azure Monitor should be saved in customer storage account for logs encryption
10.1.2	[Preview]: Secure Boot should be enabled on supported Windows virtual machines
10.1.2	[Preview]: vTPM should be enabled on supported virtual machines
10.1.2	SQL managed instances should use customer-managed keys to encrypt data at rest
10.1.2.1	App Service apps should only be accessible over HTTPS
10.1.2.1	App Service apps should require FTPS only
10.1.2.1	App Service apps should use the latest TLS version
10.1.2.1	Audit Windows machines that do not store passwords using reversible encryption
10.1.2.1	Automation account variables should be encrypted
10.1.2.1	Azure HDInsight clusters should use encryption in transit to encrypt communication between Azure HDInsight cluster nodes

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
10.1.2.1	Enforce SSL connection should be enabled for MySQL database servers
10.1.2.1	Enforce SSL connection should be enabled for PostgreSQL database servers
10.1.2.1	Function apps should only be accessible over HTTPS
10.1.2.1	Function apps should require FTPS only
10.1.2.1	Function apps should use the latest TLS version
10.1.2.1	Kubernetes clusters should be accessible only over HTTPS
10.1.2.1	Only secure connections to your Azure Cache for Redis should be enabled
10.1.2.1	Secure transfer to storage accounts should be enabled
10.1.2.1	Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign
10.1.2.1	Transparent Data Encryption on SQL databases should be enabled
10.1.2.1	Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources
10.1.2.1	Windows web servers should be configured to use secure communication protocols
12.2.1	Adaptive application controls for defining safe applications should be enabled on your machines
12.2.1	Allowlist rules in your adaptive application control policy should be updated
12.2.1	System updates on virtual machine scale sets should be installed
12.2.1	System updates should be installed on your machines
12.2.1	Azure Web Application Firewall should be enabled for Azure Front Door entry-points
12.2.1	Subscriptions should have a contact email address for security issues
12.2.1	Azure DDoS Protection Standard should be enabled
12.2.1	[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed
12.2.1	Email notification to subscription owner for high severity alerts should be enabled
12.2.1	Function apps should use latest “HTTP Version”
12.2.1	Endpoint protection solution should be installed on virtual machine scale sets
12.2.1	Monitor missing Endpoint Protection in Azure Security Center
12.2.1	IP Forwarding on your virtual machine should be disabled
12.2.1	SQL servers on machines should have vulnerability findings resolved

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
12.2.1	Vulnerabilities in container security configurations should be remediated
12.2.1	Vulnerabilities in security configuration on your machines should be remediated
12.2.1	Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
12.2.1	Azure Defender for SQL should be enabled for unprotected PostgreSQL flexible servers
12.2.1	Microsoft Defender for SQL should be enabled for unprotected Synapse workspaces
12.2.1	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version
12.2.1	Machines should be configured to periodically check for missing system updates
12.2.1	A vulnerability assessment solution should be enabled on your virtual machines
12.2.1	Azure Defender for App Service should be enabled
12.2.1	Azure Defender for Azure SQL Database servers should be enabled
12.2.1	Azure Defender for DNS should be enabled
12.2.1	Azure Defender for Key Vault should be enabled
12.2.1	Azure Defender for Resource Manager should be enabled
12.2.1	Azure Defender for servers should be enabled
12.2.1	Azure Defender for SQL servers on machines should be enabled
12.2.1	Azure Defender for SQL should be enabled for unprotected Azure SQL servers
12.2.1	Azure Defender for SQL should be enabled for unprotected SQL Managed Instances
12.2.1	Container registry images should have vulnerability findings resolved
12.2.1	Microsoft Defender for Containers should be enabled
12.2.1	Running container images should have vulnerability findings resolved
12.2.1	Vulnerability assessment should be enabled on SQL Managed Instance
12.2.1	Vulnerability assessment should be enabled on your SQL servers
12.2.1	Web Application Firewall (WAF) should be enabled for Application Gateway
12.2.1	Windows Defender Exploit Guard should be enabled on your machines
12.2.1.3	Adaptive application controls for defining safe applications should be enabled on your machines
12.2.1.3	Allowlist rules in your adaptive application control policy should be updated

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
12.2.1.3	System updates on virtual machine scale sets should be installed
12.2.1.3	System updates should be installed on your machines
12.2.1.3	Azure Web Application Firewall should be enabled for Azure Front Door entry-points
12.2.1.3	Subscriptions should have a contact email address for security issues
12.2.1.3	Azure DDoS Protection Standard should be enabled
12.2.1.3	[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed
12.2.1.3	Email notification to subscription owner for high severity alerts should be enabled
12.2.1.3	Function apps should use latest “HTTP Version”
12.2.1.3	Endpoint protection solution should be installed on virtual machine scale sets
12.2.1.3	Monitor missing Endpoint Protection in Azure Security Center
12.2.1.3	IP Forwarding on your virtual machine should be disabled
12.2.1.3	SQL servers on machines should have vulnerability findings resolved
12.2.1.3	Vulnerabilities in container security configurations should be remediated
12.2.1.3	Vulnerabilities in security configuration on your machines should be remediated
12.2.1.3	Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
12.2.1.3	Azure Defender for SQL should be enabled for unprotected PostgreSQL flexible servers
12.2.1.3	Microsoft Defender for SQL should be enabled for unprotected Synapse workspaces
12.2.1.3	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version
12.2.1.3	Machines should be configured to periodically check for missing system updates
12.2.1.3	A vulnerability assessment solution should be enabled on your virtual machines
12.2.1.3	Azure Defender for App Service should be enabled
12.2.1.3	Azure Defender for Azure SQL Database servers should be enabled
12.2.1.3	Azure Defender for DNS should be enabled
12.2.1.3	Azure Defender for Key Vault should be enabled
12.2.1.3	Azure Defender for Resource Manager should be enabled
12.2.1.3	Azure Defender for servers should be enabled

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
12.2.1.3	Azure Defender for SQL servers on machines should be enabled
12.2.1.3	Azure Defender for SQL should be enabled for unprotected Azure SQL servers
12.2.1.3	Azure Defender for SQL should be enabled for unprotected SQL Managed Instances
12.2.1.3	Container registry images should have vulnerability findings resolved
12.2.1.3	Microsoft Defender for Containers should be enabled
12.2.1.3	Running container images should have vulnerability findings resolved
12.2.1.3	Vulnerability assessment should be enabled on SQL Managed Instance
12.2.1.3	Vulnerability assessment should be enabled on your SQL servers
12.2.1.3	Web Application Firewall (WAF) should be enabled for Application Gateway
12.2.1.3	Windows Defender Exploit Guard should be enabled on your machines
12.2.1.5	Microsoft Defender for SQL should be enabled for unprotected Synapse workspaces
12.2.1.5	Azure Defender for SQL should be enabled for unprotected PostgreSQL flexible servers
12.2.1.5	Machines should be configured to periodically check for missing system updates
12.2.1.5	Subscriptions should have a contact email address for security issues
12.2.1.5	Email notification to subscription owner for high severity alerts should be enabled
12.2.1.5	Adaptive application controls for defining safe applications should be enabled on your machines
12.2.1.5	Allowlist rules in your adaptive application control policy should be updated
12.2.1.5	[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed
12.2.1.5	A vulnerability assessment solution should be enabled on your virtual machines
12.2.1.5	Azure DDoS Protection Standard should be enabled
12.2.1.5	Azure Defender for App Service should be enabled
12.2.1.5	Azure Defender for Azure SQL Database servers should be enabled
12.2.1.5	Azure Defender for DNS should be enabled
12.2.1.5	Azure Defender for Key Vault should be enabled
12.2.1.5	Azure Defender for Resource Manager should be enabled
12.2.1.5	Azure Defender for servers should be enabled

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
12.2.1.5	Azure Defender for SQL servers on machines should be enabled
12.2.1.5	Azure Defender for SQL should be enabled for unprotected Azure SQL servers
12.2.1.5	Azure Defender for SQL should be enabled for unprotected SQL Managed Instances
12.2.1.5	Azure Web Application Firewall should be enabled for Azure Front Door entry-points
12.2.1.5	Container registry images should have vulnerability findings resolved
12.2.1.5	Endpoint protection solution should be installed on virtual machine scale sets
12.2.1.5	Function apps should use latest “HTTP Version”
12.2.1.5	IP Forwarding on your virtual machine should be disabled
12.2.1.5	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version
12.2.1.5	Microsoft Defender for Containers should be enabled
12.2.1.5	Monitor missing Endpoint Protection in Azure Security Center
12.2.1.5	Running container images should have vulnerability findings resolved
12.2.1.5	SQL servers on machines should have vulnerability findings resolved
12.2.1.5	System updates on virtual machine scale sets should be installed
12.2.1.5	System updates should be installed on your machines
12.2.1.5	Vulnerabilities in container security configurations should be remediated
12.2.1.5	Vulnerabilities in security configuration on your machines should be remediated
12.2.1.5	Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
12.2.1.5	Vulnerability assessment should be enabled on SQL Managed Instance
12.2.1.5	Vulnerability assessment should be enabled on your SQL servers
12.2.1.5	Web Application Firewall (WAF) should be enabled for Application Gateway
12.2.1.5	Windows Defender Exploit Guard should be enabled on your machines
12.3.1	Azure Backup should be enabled for Virtual Machines
12.3.1	Audit virtual machines without disaster recovery configured
12.3.1	Key vaults should have deletion protection enabled
12.3.1	Key vaults should have soft delete enabled

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
12.3.1.3	Azure Backup should be enabled for Virtual Machines
12.3.1.3	Audit virtual machines without disaster recovery configured
12.3.1.3	Key vaults should have deletion protection enabled
12.3.1.3	Key vaults should have soft delete enabled
12.3.1.4	Geo-redundant backup should be enabled for Azure Database for MariaDB
12.3.1.4	Geo-redundant backup should be enabled for Azure Database for MySQL
12.3.1.4	Geo-redundant backup should be enabled for Azure Database for PostgreSQL
12.4.1	Audit diagnostic setting for selected resource types
12.4.1	[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed
12.4.1	Dependency agent should be enabled for listed virtual machine images
12.4.1	Dependency agent should be enabled in virtual machine scale sets for listed virtual machine images
12.4.1	Guest Configuration extension should be installed on your machines
12.4.1	Virtual machines' Guest Configuration extension should be deployed with system-assigned managed identity
12.4.1	Linux Arc-enabled machines should have Azure Monitor Agent installed
12.4.1	Linux virtual machine scale sets should have Azure Monitor Agent installed
12.4.1	Linux virtual machines should have Azure Monitor Agent installed
12.4.1	Windows virtual machines should have Azure Monitor Agent installed
12.4.1	Windows Arc-enabled machines should have Azure Monitor Agent installed
12.4.1	Windows virtual machine scale sets should have Azure Monitor Agent installed
12.4.1	Auditing on SQL server should be enabled
12.4.1	Auto provisioning of the Log Analytics agent should be enabled on your subscription
12.4.1	Log Analytics agent should be installed on your virtual machine for Azure Security Center monitoring
12.4.1	[Preview]: Log Analytics Extension should be enabled for listed virtual machine images
12.4.1	[Preview]: Log Analytics extension should be installed on your Linux Azure Arc machines
12.4.1	[Preview]: Log Analytics extension should be installed on your Windows Azure Arc machines
12.4.1	Log Analytics extension should be enabled in virtual machine scale sets for listed virtual machine images

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
12.4.1	[Preview]: Network traffic data collection agent should be installed on Linux virtual machines
12.4.1	[Preview]: Network traffic data collection agent should be installed on Windows virtual machines
12.4.1	App Service apps should have resource logs enabled
12.4.1	Azure Front Door Standard or Premium (Plus WAF) should have resource logs enabled
12.4.1	Azure Front Door should have Resource logs enabled
12.4.1	Resource logs in Azure Data Lake Store should be enabled
12.4.1	Resource logs in Azure Databricks Workspaces should be enabled
12.4.1	Resource logs in Azure Kubernetes Service should be enabled
12.4.1	Resource logs in Azure Machine Learning Workspaces should be enabled
12.4.1	Resource logs in Azure Stream Analytics should be enabled
12.4.1	Resource logs in Batch accounts should be enabled
12.4.1	Resource logs in Data Lake Analytics should be enabled
12.4.1	Resource logs in Event Hub should be enabled
12.4.1	Resource logs in IoT Hub should be enabled
12.4.1	Resource logs in Key Vault should be enabled
12.4.1	Resource logs in Logic Apps should be enabled
12.4.1	Resource logs in Search services should be enabled
12.4.1	Resource logs in Service Bus should be enabled
12.4.1	Network Watcher should be enabled
12.4.1	Azure Defender for App Service should be enabled
12.4.1	Azure Defender for Azure SQL Database servers should be enabled
12.4.1	Azure Defender for DNS should be enabled
12.4.1	Azure Defender for Key Vault should be enabled
12.4.1	Azure Defender for Resource Manager should be enabled
12.4.1	Azure Defender for servers should be enabled
12.4.1	Azure Defender for SQL servers on machines should be enabled

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
12.4.1	Azure Defender for SQL should be enabled for unprotected Azure SQL servers
12.4.1	Azure Defender for SQL should be enabled for unprotected SQL Managed Instances
12.4.1	Microsoft Defender for Containers should be enabled
12.6.1	Kubernetes clusters should disable automounting API credentials
12.6.1	System updates on virtual machine scale sets should be installed
12.6.1	System updates should be installed on your machines
12.6.1	Azure Policy Add-on for Kubernetes service (AKS) should be installed and enabled on your clusters
12.6.1	App Service apps should not have CORS configured to allow every resource to access your apps
12.6.1	Function apps should not have CORS configured to allow every resource to access your apps
12.6.1	App Service apps should use latest “HTTP Version”
12.6.1	Function apps should use latest “HTTP Version”
12.6.1	Endpoint protection solution should be installed on virtual machine scale sets
12.6.1	Monitor missing Endpoint Protection in Azure Security Center
12.6.1	Kubernetes cluster containers should only use allowed AppArmor profiles
12.6.1	Kubernetes cluster containers should only use allowed capabilities
12.6.1	Kubernetes cluster containers should only use allowed images
12.6.1	App Service apps should have remote debugging turned off
12.6.1	Function apps should have remote debugging turned off
12.6.1	SQL servers on machines should have vulnerability findings resolved
12.6.1	Vulnerabilities in container security configurations should be remediated
12.6.1	Vulnerabilities in security configuration on your machines should be remediated
12.6.1	Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
12.6.1	Kubernetes cluster containers CPU and memory resource limits should not exceed the specified limits
12.6.1	Kubernetes cluster services should listen only on allowed ports
12.6.1	Kubernetes cluster containers should not share host process ID or host IPC namespace
12.6.1	Kubernetes clusters should not use the default namespace

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
12.6.1	Kubernetes clusters should not grant CAP_SYS_ADMIN security capabilities
12.6.1	Kubernetes clusters should not allow container privilege escalation
12.6.1	Kubernetes cluster should not allow privileged containers
12.6.1	Kubernetes cluster containers should run with a read only root file system
12.6.1	Kubernetes cluster pods should only use approved host network and port range
12.6.1	Kubernetes cluster pod hostPath volumes should only use allowed host paths
12.6.1	Kubernetes cluster pods and containers should only run with approved user and group IDs
12.6.1	App Service apps that use Java should use a specified “Java version”
12.6.1	App Service apps that use PHP should use a specified “PHP version”
12.6.1	App Service apps that use Python should use a specified “Python version”
12.6.1	Function apps that use Java should use a specified “Java version”
12.6.1	Function apps that use Python should use a specified “Python version”
12.6.1	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version
12.6.1	Azure registry container images should have vulnerabilities resolved (powered by Microsoft Defender Vulnerability Management)
12.6.1	A vulnerability assessment solution should be enabled on your virtual machines
12.6.1	A vulnerability assessment solution should be enabled on your virtual machines
12.6.1	Azure Defender for App Service should be enabled
12.6.1	Azure Defender for Azure SQL Database servers should be enabled
12.6.1	Azure Defender for DNS should be enabled
12.6.1	Azure Defender for Key Vault should be enabled
12.6.1	Azure Defender for Resource Manager should be enabled
12.6.1	Azure Defender for servers should be enabled
12.6.1	Azure Defender for SQL servers on machines should be enabled
12.6.1	Microsoft Defender for Containers should be enabled
12.6.1	SQL databases should have vulnerability findings resolved
12.6.1	Windows Defender Exploit Guard should be enabled on your machines

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
12.6.1.1	System updates on virtual machine scale sets should be installed
12.6.1.1	System updates should be installed on your machines
12.6.1.1	App Service apps should use latest “HTTP Version”
12.6.1.1	Function apps should use latest “HTTP Version”
12.6.1.1	Endpoint protection solution should be installed on virtual machine scale sets
12.6.1.1	Monitor missing Endpoint Protection in Azure Security Center
12.6.1.1	SQL servers on machines should have vulnerability findings resolved
12.6.1.1	Vulnerabilities in container security configurations should be remediated
12.6.1.1	Vulnerabilities in security configuration on your machines should be remediated
12.6.1.1	Vulnerabilities in security configuration on your virtual machine scale sets should be remediated
12.6.1.1	App Service apps that use Java should use a specified “Java version”
12.6.1.1	App Service apps that use PHP should use a specified “PHP version”
12.6.1.1	App Service apps that use Python should use a specified “Python version”
12.6.1.1	Function apps that use Java should use a specified “Java version”
12.6.1.1	Function apps that use Python should use a specified “Python version”
12.6.1.1	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version
12.6.1.1	Azure registry container images should have vulnerabilities resolved (powered by Microsoft Defender Vulnerability Management)
12.6.1.1	A vulnerability assessment solution should be enabled on your virtual machines
12.6.1.1	A vulnerability assessment solution should be enabled on your virtual machines
12.6.1.1	Azure Defender for App Service should be enabled
12.6.1.1	Azure Defender for Azure SQL Database servers should be enabled
12.6.1.1	Azure Defender for DNS should be enabled
12.6.1.1	Azure Defender for Key Vault should be enabled
12.6.1.1	Azure Defender for Resource Manager should be enabled
12.6.1.1	Azure Defender for servers should be enabled
12.6.1.1	Azure Defender for SQL servers on machines should be enabled

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
12.6.1.1	Microsoft Defender for Containers should be enabled
12.6.1.1	SQL databases should have vulnerability findings resolved
12.6.1.1	Vulnerability assessment should be enabled on your Synapse workspaces
12.6.1.1	Windows Defender Exploit Guard should be enabled on your machines
12.6.2	Adaptive application controls for defining safe applications should be enabled on your machines
12.6.2	Allowlist rules in your adaptive application control policy should be updated
13.1.1	Adaptive network hardening recommendations should be applied on internet facing virtual machines
12.6.2.1	Azure Defender for servers should be enabled
12.6.2.1	Adaptive application controls for defining safe applications should be enabled on your machines
12.6.2.1	Allowlist rules in your adaptive application control policy should be updated
13.1.1	Azure Key Vault should have firewall enabled
13.1.1	Azure Cosmos DB accounts should have firewall rules
13.1.1	Authorized IP ranges should be defined on Kubernetes Services
13.1.1	API Management services should use a virtual network
13.1.1	Azure Databricks Workspaces should be in a virtual network
13.1.1	Azure Machine Learning Computes should be in a virtual network
13.1.1	IP Forwarding on your virtual machine should be disabled
13.1.1	Management ports of virtual machines should be protected with just-in-time network access control
13.1.1	Management ports should be closed on your virtual machines
13.1.1	Internet-facing virtual machines should be protected with network security groups
13.1.1	Subnets should be associated with a Network Security Group
13.1.1	Non-internet-facing virtual machines should be protected with network security groups
13.1.1	All network ports should be restricted on network security groups associated to your virtual machine
13.1.1	Cognitive Services accounts should restrict network access
13.1.1	Azure AI Services resources should restrict network access
13.1.1	Private endpoint connections on Azure SQL Database should be enabled

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
13.1.1	Private endpoint should be enabled for MariaDB servers
13.1.1	Private endpoint should be enabled for MySQL servers
13.1.1	Private endpoint should be enabled for PostgreSQL servers
13.1.1	Azure Databricks Clusters should disable public IP
13.1.1	Azure Cognitive Search services should disable public network access
13.1.1	Azure Cosmos DB should disable public network access
13.1.1	Azure Databricks Workspaces should disable public network access
13.1.1	Azure Machine Learning Workspaces should disable public network access
13.1.1	Azure SQL Managed Instances should disable public network access
13.1.1	Cognitive Services accounts should disable public network access
13.1.1	Public network access on Azure SQL Database should be disabled
13.1.1	[Preview]: Storage account public access should be disallowed
13.1.1	Public network access should be disabled for MariaDB servers
13.1.1	Public network access should be disabled for MySQL servers
13.1.1	Public network access should be disabled for PostgreSQL servers
13.1.1	Container registries should not allow unrestricted network access
13.1.1	Storage accounts should restrict network access using virtual network rules
13.1.1	App Configuration should use private link
13.1.1	Azure API for FHIR should use private link
13.1.1	Azure Cache for Redis should use private link
13.1.1	Azure Cognitive Search services should use private link
13.1.1	Azure Data Factory should use private link
13.1.1	Azure Databricks Workspaces should use private link
13.1.1	Azure Event Grid domains should use private link
13.1.1	Azure Event Grid topics should use private link
13.1.1	Azure File Sync should use private link

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
13.1.1	Azure Key Vaults should use private link
13.1.1	Azure Machine Learning workspaces should use private link
13.1.1	Azure Service Bus namespaces should use private link
13.1.1	Azure SignalR Service should use private link
13.1.1	Azure Synapse workspaces should use private link
13.1.1	Azure Web PubSub Service should use private link
13.1.1	Cognitive Services should use private link
13.1.1	Container registries should use private link
13.1.1	CosmosDB accounts should use private link
13.1.1	Disk access resources should use private link
13.1.1	Event Hub namespaces should use private link
13.1.1	IoT Hub device provisioning service instances should use private link
13.1.1	Storage accounts should use private link
13.1.1	VM Image Builder templates should use private link
13.1.1	Azure Front Door profiles should use Premium tier that supports managed WAF rules and private link
13.1.1	Azure Cognitive Search service should use a SKU that supports private link
13.1.1	Storage accounts should restrict network access
13.1.1	Azure Web Application Firewall should be enabled for Azure Front Door entry-points
12.6.2	Azure Defender for servers should be enabled
13.1.1	Web Application Firewall (WAF) should be enabled for Application Gateway
13.1.2	All network ports should be restricted on network security groups associated to your virtual machine
13.1.2	Azure DDoS Protection Standard should be enabled
13.1.2	Azure Web Application Firewall should be enabled for Azure Front Door entry-points
13.1.2	IP Forwarding on your virtual machine should be disabled
13.1.2	Storage accounts should restrict network access
13.1.2	Web Application Firewall (WAF) should be enabled for Application Gateway

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
13.1.2.4	All network ports should be restricted on network security groups associated to your virtual machine
13.1.2.4	Azure DDoS Protection Standard should be enabled
13.1.2.4	Azure Web Application Firewall should be enabled for Azure Front Door entry-points
13.1.2.4	IP Forwarding on your virtual machine should be disabled
13.1.2.4	Storage accounts should restrict network access
13.1.2.4	Web Application Firewall (WAF) should be enabled for Application Gateway
17.2.1	Geo-redundant backup should be enabled for Azure Database for MariaDB
17.2.1	Geo-redundant backup should be enabled for Azure Database for MySQL
17.2.1	Geo-redundant backup should be enabled for Azure Database for PostgreSQL
17.2.1	Audit virtual machines without disaster recovery configured
17.2.1	Azure Backup should be enabled for Virtual Machines
18.1.1	Allowed Locations
18.1.1	Allowed locations for resource groups
18.1.5	Azure HDInsight clusters should use encryption at host to encrypt data at rest
18.1.5	Virtual machines and virtual machine scale sets should have encryption at host enabled
18.1.5	[Preview]: Azure Recovery Services vaults should use customer-managed keys for encrypting backup data
18.1.5	[Preview]: IoT Hub device provisioning service data should be encrypted using customer-managed keys (CMK)
18.1.5	Azure API for FHIR should use a customer-managed key to encrypt data at rest
18.1.5	Azure Automation accounts should use customer-managed keys to encrypt data at rest
18.1.5	Azure Batch account should use customer-managed keys to encrypt data
18.1.5	Azure Container Instance container group should use customer-managed key for encryption
18.1.5	Azure Cosmos DB accounts should use customer-managed keys to encrypt data at rest
18.1.5	Azure Data Box jobs should use a customer-managed key to encrypt the device unlock password
18.1.5	Azure Data Explorer encryption at rest should use a customer-managed key
18.1.5	Azure data factories should be encrypted with a customer-managed key
18.1.5	Azure HDInsight clusters should use customer-managed keys to encrypt data at rest

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
18.1.5	Azure Machine Learning workspaces should be encrypted with a customer-managed key
18.1.5	Azure Monitor Logs clusters should be encrypted with customer-managed key
18.1.5	Azure Stream Analytics jobs should use customer-managed keys to encrypt data
18.1.5	Azure Synapse workspaces should use customer-managed keys to encrypt data at rest
18.1.5	Bot Service should be encrypted with a customer-managed key
18.1.5	Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys
18.1.5	Cognitive Services accounts should enable data encryption with a customer-managed key
18.1.5	Container registries should be encrypted with a customer-managed key
18.1.5	Event Hub namespaces should use a customer-managed key for encryption
18.1.5	HPC Cache accounts should use customer-managed key for encryption
18.1.5	Logic Apps Integration Service Environment should be encrypted with customer-managed keys
18.1.5	MySQL servers should use customer-managed keys to encrypt data at rest
18.1.5	OS and data disks should be encrypted with a customer-managed key
18.1.5	PostgreSQL servers should use customer-managed keys to encrypt data at rest
18.1.5	Service Bus Premium namespaces should use a customer-managed key for encryption
18.1.5	SQL servers should use customer-managed keys to encrypt data at rest
18.1.5	Storage account encryption scopes should use customer-managed keys to encrypt data at rest
18.1.5	Storage accounts should use customer-managed key for encryption
18.1.5	Azure Batch pools should have disk encryption enabled
18.1.5	Disk encryption should be enabled on Azure Data Explorer
18.1.5	Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host
18.1.5	Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources
18.1.5	Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.
18.1.5	Linux virtual machines should enable Azure Disk Encryption or EncryptionAtHost.
18.1.5	Azure Data Box jobs should enable double encryption for data at rest on the device
18.1.5	Azure Edge Hardware Center devices should have double encryption support enabled

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
18.1.5	Azure Monitor Logs clusters should be created with infrastructure-encryption enabled (double encryption)
18.1.5	Double encryption should be enabled on Azure Data Explorer
18.1.5	Managed disks should be double encrypted with both platform-managed and customer-managed keys
18.1.5	Infrastructure encryption should be enabled for Azure Database for MySQL servers
18.1.5	Infrastructure encryption should be enabled for Azure Database for PostgreSQL servers
18.1.5	Storage accounts should have infrastructure encryption
18.1.5	Transparent Data Encryption on SQL databases should be enabled
18.1.5	[Preview]: Guest Attestation extension should be installed on supported Linux virtual machines
18.1.5	[Preview]: Guest Attestation extension should be installed on supported Windows virtual machines
18.1.5	[Preview]: Guest Attestation extension should be installed on supported Linux virtual machines scale sets
18.1.5	[Preview]: Guest Attestation extension should be installed on supported Windows virtual machines scale sets
18.1.5	Saved-queries in Azure Monitor should be saved in customer storage account for logs encryption
18.1.5	[Preview]: Secure Boot should be enabled on supported Windows virtual machines
18.1.5	[Preview]: vTPM should be enabled on supported virtual machines
18.1.5	SQL managed instances should use customer-managed keys to encrypt data at rest
18.1.5.1	Azure HDInsight clusters should use encryption at host to encrypt data at rest
18.1.5.1	Virtual machines and virtual machine scale sets should have encryption at host enabled
18.1.5.1	[Preview]: Azure Recovery Services vaults should use customer-managed keys for encrypting backup data
18.1.5.1	[Preview]: IoT Hub device provisioning service data should be encrypted using customer-managed keys (CMK)
18.1.5.1	Azure API for FHIR should use a customer-managed key to encrypt data at rest
18.1.5.1	Azure Automation accounts should use customer-managed keys to encrypt data at rest
18.1.5.1	Azure Batch account should use customer-managed keys to encrypt data
18.1.5.1	Azure Container Instance container group should use customer-managed key for encryption
18.1.5.1	Azure Cosmos DB accounts should use customer-managed keys to encrypt data at rest
18.1.5.1	Azure Data Box jobs should use a customer-managed key to encrypt the device unlock password
18.1.5.1	Azure Data Explorer encryption at rest should use a customer-managed key

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
18.1.5.1	Azure data factories should be encrypted with a customer-managed key
18.1.5.1	Azure HDInsight clusters should use customer-managed keys to encrypt data at rest
18.1.5.1	Azure Machine Learning workspaces should be encrypted with a customer-managed key
18.1.5.1	Azure Monitor Logs clusters should be encrypted with customer-managed key
18.1.5.1	Azure Stream Analytics jobs should use customer-managed keys to encrypt data
18.1.5.1	Azure Synapse workspaces should use customer-managed keys to encrypt data at rest
18.1.5.1	Bot Service should be encrypted with a customer-managed key
18.1.5.1	Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys
18.1.5.1	Cognitive Services accounts should enable data encryption with a customer-managed key
18.1.5.1	Container registries should be encrypted with a customer-managed key
18.1.5.1	Event Hub namespaces should use a customer-managed key for encryption
18.1.5.1	HPC Cache accounts should use customer-managed key for encryption
18.1.5.1	Logic Apps Integration Service Environment should be encrypted with customer-managed keys
18.1.5.1	MySQL servers should use customer-managed keys to encrypt data at rest
18.1.5.1	OS and data disks should be encrypted with a customer-managed key
18.1.5.1	PostgreSQL servers should use customer-managed keys to encrypt data at rest
18.1.5.1	Service Bus Premium namespaces should use a customer-managed key for encryption
18.1.5.1	SQL servers should use customer-managed keys to encrypt data at rest
18.1.5.1	Storage account encryption scopes should use customer-managed keys to encrypt data at rest
18.1.5.1	Storage accounts should use customer-managed key for encryption
18.1.5.1	Azure Batch pools should have disk encryption enabled
18.1.5.1	Disk encryption should be enabled on Azure Data Explorer
18.1.5.1	Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host
18.1.5.1	Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources
18.1.5.1	Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.
18.1.5.1	Linux virtual machines should enable Azure Disk Encryption or EncryptionAtHost.

IO Control/ Overheids-maatregel	Settings BIO Compliance Initiative Template (alle settings in versie 2.2.3)
18.1.5.1	Azure Data Box jobs should enable double encryption for data at rest on the device
18.1.5.1	Azure Edge Hardware Center devices should have double encryption support enabled
18.1.5.1	Azure Monitor Logs clusters should be created with infrastructure-encryption enabled (double encryption)
18.1.5.1	Double encryption should be enabled on Azure Data Explorer
18.1.5.1	Managed disks should be double encrypted with both platform-managed and customer-managed keys
18.1.5.1	Infrastructure encryption should be enabled for Azure Database for MySQL servers
18.1.5.1	Infrastructure encryption should be enabled for Azure Database for PostgreSQL servers
18.1.5.1	Storage accounts should have infrastructure encryption
18.1.5.1	Transparent Data Encryption on SQL databases should be enabled
18.1.5.1	[Preview]: Guest Attestation extension should be installed on supported Linux virtual machines
18.1.5.1	[Preview]: Guest Attestation extension should be installed on supported Windows virtual machines
18.1.5.1	[Preview]: Guest Attestation extension should be installed on supported Linux virtual machines scale sets
18.1.5.1	[Preview]: Guest Attestation extension should be installed on supported Windows virtual machines scale sets
18.1.5.1	Saved-queries in Azure Monitor should be saved in customer storage account for logs encryption
18.1.5.1	[Preview]: Secure Boot should be enabled on supported Windows virtual machines
18.1.5.1	[Preview]: vTPM should be enabled on supported virtual machines
18.1.5.1	SQL managed instances should use customer-managed keys to encrypt data at rest
N/A	App Service apps should have Client Certificates (Incoming client certificates) enabled
N/A	App Service Environment should have internal encryption enabled
N/A	Azure Front Door Standard and Premium should be running minimum TLS version of 1.2
N/A	Azure Machine Learning compute instances should be recreated to get the latest software updates
N/A	Azure SQL Database should be running TLS version 1.2 or newer
N/A	Email notification for high severity alerts should be enabled
N/A	Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring
N/A	SQL servers with auditing to storage account destination should be configured with 90 days retention or higher
N/A	Azure running container images should have vulnerabilities resolved (powered by Microsoft Defender Vulnerability Management)