Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services

Ministerie van Justitie en Veiligheid

Rapportage inzake BIO-compliance Microsoft betreffende
- Microsoft365: Teams;
- Azure: Active Directory.

20 oktober 2023

Building a better working world

Inhoudsopgave

Ernst & Young Accountants LLP
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 oktober 2023 REQ6802038/MM/ks

Rapportage fase A en B onderzoek BIO-compliance Microsoft

Geachte heer, mevrouw,

U heeft ons een adviesopdracht gegeven tot het onderzoeken van de mate van compliance van Microsoft-diensten in relatie tot de Baseline Informatiebeveiliging Overheid (hierna BIO), op basis van reeds aanwezige assurance rapportages over deze diensten. Hierbij is ook specifieke aandacht gevraagd voor de wijze waarop Microsoft-producten eventueel geconfigureerd moeten worden om deze BIO-compliant te gebruiken. Conform uw opdracht brengen wij bijgaand onze adviesrapportage uit.

Het concept van deze rapportage is met u en de klankbordgroep afgestemd en 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 beoordelings-opdracht en deze resulteert dan ook niet in een assurance rapportage.

Deze rapportage is alleen bestemd voor de beoogde gebruikers, zoals is vastgelegd in de 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,
Ernst & Young Accountants LLP

Peter Kornelisse
Digitally signed by Peter Kornelisse
DN: cn=Peter Kornelisse, c=NL, o=Ernst & Young Accountants LLP
Date: 2023.10.20 17:23:07 +02'00'

Maarten Muurling
Digitally signed by Maarten Muurling
DN: cn=Maarten Muurling, c=NL, o=Ernst & Young Accountants LLP
Date: 2023.10.20 16:07:02 +02'00'

Peter Kornelisse
Partner

Maarten Muurling
Partner

1 Inleiding

1.1 Ontzorgen van gebruikersorganisaties

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 ontzorgen betreffende het voldoen aan de BIO bij gebruik van producten van Microsoft, is het van belang dat organisaties binnen de Nederlandse overheid goed zijn geïnformeerd over de mate waarin deze producten voldoen aan de BIO op basis van BBN2 (basisbeveiligingsniveau 2). Zoals in de BIO staat beschreven, vormt BBN2 het uitgangspunt voor informatiesystemen binnen de overheid. BBN2 is van toepassing indien:

- Vertrouwelijke informatie wordt verwerkt.
- Mogelijke incidenten leiden tot bestuurlijke commotie.
- De veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.

In de BIO zijn hiertoe opgenomen:

- BIO-controls (conform de opbouw van ISO-27002).
- 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). Tevens 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 van Hyperscalers. Dit betreft met name het laten uitvoeren van:

- DPIA's
- (Technische) verificatieonderzoeken
- Audits.

Kenmerkend voor deze audits is dat bij Hyperscalers 'onder de motorkap' onderzoek kan plaatsvinden en vervolgens hierover mogelijke assurance-werkzaamheden uitgevoerd kunnen worden.

Het voorliggende rapport betreft een onderzoek naar de mate waarin voldaan wordt aan de BIO bij het gebruik van de diensten van Microsoft. Hiertoe is onderzocht welke rapportages over de in scope zijnde diensten reeds beschikbaar zijn: assurance rapportages (SOC), FedRAMP-rapportages, ISO27001-certificering.

2 Opdracht

2.1 Achterliggende vraagstelling

SLM heeft ons gevraagd een onderzoek uit te voeren bij Microsoft betreffende de volgende vraag:

> *"In hoeverre en op welke wijze zijn de producten en diensten van Microsoft die worden afgenomen BIO-compliant te gebruiken?"*

2.2 Doelstelling van de opdracht

Het doel van deze opdracht is het onderzoeken van en rapporteren over de mate waarin reeds assurance beschikbaar is over het voldoen aan de BIO (Baseline Informatiebeveiliging Overheid 1.04zv 17-06-2020) bij gebruik van Microsoft-diensten door overheden. Hiertoe wordt gebruikgemaakt van rapportages over Microsoft-diensten zoals opgenomen op de Microsoft Service Trust Portal. Als onderdeel van de werkzaamheden wordt tevens inzicht gegeven in maatregelen die overheden zelf dienen te treffen.

2.3 Reikwijdte en afbakening

De reikwijdte van ons onderzoek betreft de dekking van de BIO-controls en -overheidsmaatregelen in aanwezige assurance rapportages (SOC), en/of aanwezig zijn in rapportages, certificeringen en raamwerken betreffende FEDRAMP, ISO27001, en NIST, voor de volgende Microsoft-diensten:

- M365: Teams
- Azure: Active Directory (hierna: Azure AD)

De hiertoe relevante assurance rapportages in de Microsoft Service Trust Portal betreffen:

- M365: Microsoft Corporation– Microsoft Office365 System and Organization Controls (SOC) 2 Report October 1, 2020, through September 30, 2021.
- Azure: Microsoft Corporation - Azure Including Dynamics 365 (Azure & Azure Government) System and Organization Controls (SOC) 2 Report October 1, 2020 - September 30, 2021).

2.4 Van toepassing zijnde normen

Het onderzoeken van BIO-compliance vindt plaats op basis van normen uit de BIO. Deze normen betreffen:

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

Voor de van toepassing zijnde normen is onderzocht in hoeverre controls aanwezig zijn in assurance rapportages (SOC), FedRAMP-rapportages en ISO27001-certificeringen.

- Assurance rapportages (SOC) betreffen de uitkomsten van toetsingswerkzaamheden conform internationale assurance-standaarden. Dit betreffen dan ook internationaal erkende assurance rapportages. De basis voor de toetsingswerkzaamheden wordt gevormd door gehanteerde beheersdoelstellingen en -maatregelen zoals gedefinieerd door Microsoft, evenals de naleving daarvan.

- FedRAMP (Federal Risk and Authorization Management Program)-rapportages betreffen de uitkomsten van toetsingswerkzaamheden die conform de FedRAMP-standaarden van de overheid van de Verenigde Staten (VS) zijn uitgevoerd en zijn een voorwaarde voor cloud service providers om diensten aan de (federale) overheid in de VS te mogen leveren. Bij FedRAMP worden de frequentie en diepgang van toetsingswerkzaamheden bepaald op basis van het risico waarop een beheersmaatregel betrekking heeft. De basis voor deze toetsingswerkzaamheden betreft een standaard set aan beveiligings- en beheersmaatregelen, die zijn opgesteld door de Amerikaanse Federal Government, gebaseerd op standaarden van NIST (National Institute of Standards and Technology) en FISMA (Federal Information Security Management Act). Deze rapportages zijn niet internationaal erkend als assurance rapportages. Hierbij is het goed om op te merken dat wij niet de rapportages zelf ontvangen hebben, maar het Systems Security Plan (hierna: SSP) wat getoetst wordt ten behoeve van de FedRAMP rapportage. Gezien het feit dat Microsoft tot op heden de FedRAMP-autorisatie heeft behouden, kan hieruit afgeleid worden dat Microsoft voldoende heeft gepresteerd bij deze audits, derhalve staat dit in de toelichting bij de uitkomsten vermeld als 'FedRAMP-rapportage'.

- Microsoft beschikt over een eigen controleraamwerk dat onder meer is gebaseerd op de beheersmaatregelen (controls) uit het NIST 800 53A Rev.4-raamwerk. Dit raamwerk wordt gebruikt binnen zowel M365 als Azure ten behoeve van het beheersen van security- en privacy-risico's. Beheersmaatregelen uit dit eigen raamwerk worden in opdracht van Microsoft door onafhankelijke partijen getoetst, bijvoorbeeld op basis van ISO 27001:2013, ISAE SOC2 en FedRAMP.

Vanwege de wisselende frequentie en diepgang van toetsing (op basis van het onderkende risico) bij SOC- en FedRAMP-rapportages is het niet mogelijk een éénduidige vergelijking te maken van de mate van zekerheid die verkregen wordt op basis van deze verschillende toetsingswerkzaamheden. Voor FedRAMP-autorisatie is het bijvoorbeeld noodzakelijk dat na de initiële beoordeling een proces voor continue monitoring is ingericht. Vervolgens dient op basis van uitgevoerde controles periodiek te worden gerapporteerd en dient minimaal jaarlijks een assessment-rapportage door een onafhankelijke derde partij te worden uitgebracht. Deze rapportage heeft betrekking op een gedefinieerde subset van beheersmaatregelen, evenals een aanvullende, wisselende selectie van beheersmaatregelen die door de 'authorizing official' wordt geselecteerd. Voor meer informatie over FedRAMP en het proces van continue monitoring verwijzen wij naar de publiek beschikbare informatie op: https://www.FedRAMP.gov en https://www.FedRAMP.gov/assets/resources/documents/CSP_Continuous_Monitoring_Strategy_Guide.pdf

De voor dit onderzoek gebruikte documentatie, zoals door ons verkregen vanuit de Microsoft Service Trust Portal, betreft:

Microsoftdienst	Soort documentatie	Betrokken partij	Documentnaam
Algemeen	Bijlage bij productvoorwaarden	Microsoft	Bijlage Bescherming van persoonsgegevens voor Producten en Diensten van Microsoft (laatst bijgewerkt op 15-09-2021).
Office365	ISAE3402 Type II (SOC)	Deloitte & Touche LLP	Microsoft Office365 System and Organization Controls (SOC) 2 Report October 1, 2020, through September 30, 2021.

Microsoftdienst	Soort documentatie	Betrokken partij	Documentnaam
Office365	ISO27001 statement of applicability en certificaat	BSI	Office365 - Audited Controls ISO 27001_2013; Microsoft M365 ISO IEC 27001-2013 (2022-2025).
Office365	FedRAMP	Coalfire Systems, Inc.	Office365 - MT - FedRAMP SSP v9.1 (2021).
Azure	ISAE3402 Type II (SOC)	Deloitte & Touche LLP	Azure Including Dynamics 365 (Azure & Azure Government) System and Organization Controls (SOC) 2 Report October 1, 2020 - September 30, 2021.
Azure	ISO27001 statement of applicability en certificaat	Schellman & Company, LLC	Azure Control Framework_Customer_V 1.0 Microsoft Azure, Dynamics and Online Services - ISO 27001 Certificate (with UKAS) 7.1.2022.pdf.
Azure	FedRAMP	Kratos	Azure - Commercial System Security Plan (SSP) v3.6 (2020).

Deze rapportages zijn voor gebruikers van de Microsoft-services te vinden in het Microsoft Service Trust Portal (https://servicetrust.microsoft.com/). Voor de ISO-control mapping wordt verwezen naar de purview compliance manager (https://learn.microsoft.com/en-us/purview/compliance-manager-templates-list?source=recommendations).

2.5 Beperkingen

Onze dienstverlening 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. Dit betreft ook geen assurance met betrekking tot financiële verslaggeving, jaarrekeningen of overige financiële informatie als onderdeel van onze dienstverlening.

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

- Het geven van een oordeel over de juistheid van BIO-controls, -overheidsmaatregelen of assurance rapportages betreffende Microsoft.
- Het geven van een oordeel over de toereikendheid van BIO-controls, -overheidsmaatregelen of assurance rapportages betreffende Microsoft.
- Het geven van een oordeel over het voldoen aan BIO-controls of -overheidsmaatregelen.

Wij zullen geen fouten en/of gebreken ten aanzien van uw computersystemen, overige apparatuur dan wel onderdelen daarvan (hierna te noemen: Systemen) signaleren, aan de orde stellen, herstellen of oplossen, ongeacht of deze te wijten zijn aan onnauwkeurige of onduidelijke invoer, opslag, interpretatie of verwerking of rapportage van informatie. Wij zijn niet verantwoordelijk voor gebreken of problemen die voortvloeien uit of verband houden met gegevensverwerking in bepaalde systemen.

Gebruik van de rapportage

De beoogde gebruikers van deze rapportage zijn de overheidsorganisaties die een overeenkomst afgesloten hebben met Microsoft voor M365 en/of Azure AD onder de overheden die verplicht zijn de BIO toe te passen. Het doel van deze opdracht is het geven van inzicht over de mate waarin reeds assurance beschikbaar is over het voldoen aan de BIO bij gebruik van Microsoft-diensten door overheden.

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.

3 Werkwijze

3.1 Organisatie

Bij het uitvoeren van deze opdracht zijn naast EY verschillende groepen stakeholders betrokken, een werkgroep, een klankbordgroep en SLM als opdrachtgever. De werkgroep bestaat uit een vertegenwoordiging van CISO's vanuit de Rijksoverheid samen met EY. De werkzaamheden van de werkgroep bestaan uit het afstemmen van verantwoordelijkheden bij de verschillende partijen en afstemming van de afwegingen die EY opstelt op basis van de beschikbare assurance rapportages en aanvullende informatie. Tevens doet de werkgroep een voorstel voor het verkrijgen van aanvullende informatie betreffende de overheidsmaatregelen waarvoor de thans beschikbare assurance rapportages niet toereikend zijn om met redelijke mate van zekerheid vast te stellen dat aan BIO-compliance wordt voldaan. Met SLM vindt formele besluitvorming plaats omtrent de scope van de opdracht, accorderen van voorstellen door de werkgroep en afstemmen van de concept assurance rapportage.

3.2 Aanpak

3.2.1 Fasering van werkzaamheden

Onze werkzaamheden zijn dusdanig opgebouwd, dat uiteindelijk assurance zou kunnen worden geleverd betreffende het voldoen aan BIO-compliance voor in scope zijnde diensten van Microsoft. Hiertoe vinden werkzaamheden plaats in vier fasen:

- A. Vraag en behoefte, waarin de scope van de gevraagde assurance-werkzaamheden verkend en een analyse op beschikbare documentatie plaatsvindt.
- B. Vaststelling scope, waarin inzichtelijk wordt gemaakt voor welke BIO-normen assurance beschikbaar is, zodat SLM kan bepalen op welke normen aanvullende assurance gewenst is.
- C. Vastelling controleraamwerk, waarbij voor de controls waarvoor aanvullende assurance gewenst is, bepaald wordt welke beheersmaatregelen bij Microsoft aanwezig zijn om aanvullende assurance te verkrijgen.
- D. Uitvoering onderzoek, waarbij een audit wordt uitgevoerd op de door SLM geselecteerde normen van Microsoft.

Het voorliggende document betreft de uitkomsten van de fasen A en B. Op basis van de reeds beschikbaar gekomen dekkende assurance- en overige compliance-informatie ziet SLM geen aanleiding de fasen C en D uit te laten voeren.

3.2.2 Onderzoeken per norm

Per norm, ofwel per BIO-control en -overheidsmaatregel, is eerst bepaald welke de verantwoordelijke organisaties zijn om te voldoen aan BIO-compliance, waarbij drie uitkomsten mogelijk waren:

- Verantwoordelijkheid ligt bij de Leverancier (Microsoft beheer van Azure AD en M365).
- Verantwoordelijkheid ligt bij de Afnemer van de betreffende diensten:
  1) Bij de *tenant-beheerder* (bijvoorbeeld een shared serviceorganisatie), en/of:
  2) Bij de *gebruikersorganisatie*.

Vervolgens is onderzocht voor elk van de BIO-normen onder verantwoordelijkheid van Microsoft (verantwoordelijkheid ligt bij de leverancier) of deze BIO-controls opgenomen zijn in bestaande assurance

rapportages betreffende Microsoft-diensten. Let op, dit betekent ook dat enkele normen voor Microsoft niet van toepassing zijn.

Daarbij is per norm (BIO-control en -overheidsmaatregel) onderzocht in hoeverre deze expliciet zijn onderkend als onderdeel van de in de assurance rapportages (SOC) en/of FedRAMP-rapportages, evenals het ISO27001/NIST-raamwerk, waarbij de uitkomst is:

1. Controls aanwezig in assurance rapportage (SOC) of control is niet (geheel) gedekt maar geaccepteerd door werkgroep.
    a. Overheidsmaatregel is expliciet afgedekt door control(s) in assurance rapportage.
    b. Geen controls aanwezig in assurance rapportage (SOC), ontbreken van assurance geaccepteerd door werkgroep.
    Overheidsmaatregel of control is NIET expliciet afgedekt door control(s) in assurance rapportage, maar het risico is geaccepteerd door de werkgroep op basis van aanvullend ontvangen informatie dan wel aangezien geen aanvullende zekerheid verkregen wordt door het toetsen van de specifieke control of beheersmaatregel.
2. Controls aanwezig in FedRAMP-rapportage
    De betreffende BIO-control/overheidsmaatregel is aanwezig in de beschikbaar gestelde FedRAMP-rapportage.
3. Controls aanwezig in ISO27001/NIST-raamwerk Microsoft
    De betreffende BIO-control/overheidsmaatregel is aanwezig in het beschikbaar gestelde ISO27001/NIST raamwerk.
4. Geen controls beschreven
    Op basis van thans beschikbare assurance en FedRAMP-rapportages evenals overige ontvangen informatie kan niet wordt vastgesteld dat specifieke controls omtrent de BIO-norm of maatregelen geformuleerd zijn.

Tot slot is per BIO-control en -overheidsmaatregel bepaald of de gebruikersorganisatie volgens Microsoft een zogenoemde CUEC (Complementary User Entity Controls, oftewel eindgebruikersmaatregelen) dient in te richten, of verhoogde aandacht dient te hebben om de dienst op een juiste wijze te configureren.

4 Managementsamenvatting

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

> *"In hoeverre en op welke wijze zijn de producten en diensten van Microsoft die worden afgenomen BIO-compliant te gebruiken?"*

Om deze onderzoeksvraag te beantwoorden is per BIO-control en BIO-overheidsmaatregel voor zowel M365 (Teams) als Azure (AD) onderzocht in welke mate beheersmaatregelen (controls) aanwezig zijn op basis van bestaande rapportages betreffende deze diensten van Microsoft. Hierbij is onderscheid te maken in:

- Controls aanwezig in assurance rapportage (SOC) of geaccepteerd door werkgroep.
- Controls aanwezig in FedRAMP-rapportage.
- Controls aanwezig in ISO27001/NIST-raamwerk Microsoft.
- Geen controls beschreven.

In de hiernavolgende tabellen zijn de kerngetallen uit het onderzoek weergegeven:

Microsoft365

Dienst	Type norm	Controls totaal	Controls aanwezig in assurance rapportage (SOC) of ontbreken geaccepteerd door werkgroep	Controls aanwezig in FedRAMP-raamwerk*	Controls aanwezig in ISO/NIST-raamwerk Microsoft**	Geen controls beschreven	n.v.t.
M365	BIO-controls	112	71	16	24	0	1
M365	BIO-overheidsmaatregelen	138	82	10	37	8	1
Subtotaal per categorie		-	153	26	61	8	2
Totaal aantal BIO-controls en overheidsmaatregelen		250					

Azure

Dienst	Type norm	Controls totaal	Controls aanwezig in Assurance (SOC) rapportage of ontbreken geaccepteerd door werkgroep	Controls aanwezig in FedRAMP-raamwerk*	Controls aanwezig in ISO-control mapping/NIST raamwerk Microsoft**	Geen controls beschreven	n.v.t.
Azure	BIO-controls	112	88	15	8	0	1
Azure	BIO-overheidsmaatregelen	138	85	7	36	9	1
Subtotaal per categorie		-	173	22	44	9	2
Totaal aantal BIO-controls en overheidsmaatregelen		250					

**= Deze controls zijn opgenomen in het eigen Microsoft-controls-raamwerk zoals beschreven in 2.4.*

***= Van Microsoft hebben wij vernomen dat de ISO-control-mapping en de onderliggende controls worden getoetst binnen een ISO-certificering, en dat het NIST-raamwerk o.a. getoetst wordt in FedRAMP en (grotendeels) in SOCII, maar niet alle direct herleidbaar. Voor die controls hebben wij de onderliggende controls in het control framework van Microsoft geïdentificeerd.*

Uit deze kerngetallen, zoals opgenomen in de tabellen, blijkt dat:

- Voor 328 normen (66%) zijn controls aanwezig in de assurance rapportages, of is het ontbreken van specifieke controls in de assurance rapportages geaccepteerd door de werkgroep (som van BIO-controls en BIO-overheidsmaatregelen voor M365 en Azure).
- Voor 43 normen (9%) zijn controls aanwezig in de FedRAMP-rapportage (som van BIO-controls en BIO-overheids-maatregelen voor M365 en Azure).
- Voor 106 normen (21%) zijn controls aanwezig in het ISO- of NIST-raamwerk (som van BIO-controls en BIO-overheids-maatregelen voor M365 en Azure).
- Voor 19 normen (4%) geen controls zijn beschreven in onafhankelijke rapportages (som van BIO-controls en BIO-overheids-maatregelen voor M365 en Azure).

Betreffende de BIO-normen waarvoor geen assurance aanwezig is, of waarvoor het risico geaccepteerd is door de werkgroep, geldt in het algemeen dat Microsoft controls heeft gedefinieerd en informatie omtrent deze controls beschikbaar is gesteld vanuit Microsoft. Dit betreft veelal ISO 27001-certificeringen en FedRAMP-beoordelingen zonder assurance.

Op basis van het door ons uitgevoerde onderzoek verdienen drie onderwerpen in het bijzonder de aandacht:

1. Er dient te worden vastgesteld in welke mate en voor welke BIO-controls en BIO-overheidsmaatregelen, waarvoor geen assurance aanwezig is of het risico niet geaccepteerd kon worden, aanvullende assurance noodzakelijk wordt geacht.
2. Indien volgens SLM aanvullende assurance noodzakelijk wordt geacht, kan deze ofwel verkregen worden in de volgende assurance rapportages van Microsoft (mits de beschreven controls daarin worden opgenomen), of door het uitvoeren van een audit op specifieke controls. Hierbij is de aanbeveling de werkzaamheden allereerst te richten op het (hogere) BIO-control niveau en eventueel, indien noodzakelijk voor het afdekken van het risico, op het meer gedetailleerde BIO-overheids-maatregelniveau.
3. Iedere overheidsorganisatie, die gebruik maakt van Microsoft, dient vast te stellen of de eigen getroffen beveiligingsmaatregelen afdoende zijn, om in samenhang met de maatregelen van Microsoft tot dekking van de BIO-controls en BIO-maatregelen te komen. Hiertoe rapporteren wij ook vereiste eindgebruikersmaatregelen in hoofdstuk 5 (onder aandachtspunten gebruikersorganisatie).

In bijlage 1 van dit rapport is de reactie van Microsoft opgenomen omtrent controls die geen onderdeel zijn van de verkregen assurance rapportages en/of raamwerken voor certificeringen. Voor de goede orde geven wij aan dat deze reactie niet inhoudelijk door ons is onderzocht.

5 Uitkomsten onderzoek

Op basis van de door ons uitgevoerde werkzaamheden zijn in dit hoofdstuk de uitkomsten van de mate waarin BIO-controls en -overheidsmaatregelen, op basis van bestaande assurance rapportages, voldoen. Hierbij is een belangrijk aandachtspunt voor de gebruikersorganisaties dat:

- Naast de BIO-controls en -overheidsmaatregelen bij Microsoft, dienen ook door overheidsorganisaties zelf relevante vereisten vanuit de BIO-intern te zijn opgezet en verantwoord. Deze vereisten worden ook wel Complementary User Entity Controls (CUEC) genoemd.
- Deze rapportage betreft een eenmalig onderzoek op basis van door Microsoft over 2021 verkregen assurance. Deze assurance dient door de gebruikersorganisatie elk jaar beoordeeld te worden. Onderstaand onderzoeksresultaten zijn is hierbij richtinggevend en kan ondersteunend zijn in het effectief en efficiënt beoordelen van de assurance
  rapportages.

5.1 Leeswijzer

Voor zover assurance aangetroffen in bestaande assurancerapportages, wordt verwezen naar controls in die assurancerapportages

Per BIO-norm is aangegeven:
- Of controls aanwezig zijn of eventueel het ontbreken van controls is geaccepteerd;
- Waar deze controls aanwezig zijn (SOC, FedRAMP, ISO/NIST raamwerken)

Indien van toepassing, dan wordt in deze kolom een verantwoordelijkheid voor de gebruikersorganisatie aangegeven

BIO-control in blauw

BIO-overheidsmaatregel in groen

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
5.1.1	**Beleidsregels voor informatiebeveiliging: Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.**	CA-17	IS-1 IS-2	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
5.1.1.1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten: a) de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid; b) de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden; c) de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers; d) de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn; e) de frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd; f) de bevordering van het beveiligingsbewustzijn.	CA-17	IS-1 IS-2	Ontbreken control in SOC geaccepteerd door werkgroep. Op basis van de beschikbare assurance rapportages is het niet mogelijk vast te stellen of alle vereiste aandachtspunten expliciet zijn opgenomen in beleid. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen significante aanvullende zekerheid geeft om beveiligingsrisico's verder te reduceren.		

5.2 Detailuitkomsten

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
5.1.1	Beleidsregels voor informatiebeveiliging: Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	CA-17	IS-1 IS-2	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
5.1.1.1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten: a) de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid; b) de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden; c) de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers; d) de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn; e) de frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd; f) de bevordering van het beveiligingsbewustzijn.	CA-17	IS-1 IS-2	Ontbreken control in SOC geaccepteerd door werkgroep. Op basis van de beschikbare assurance rapportages is het niet mogelijk vast te stellen of alle vereiste aandachtspunten expliciet zijn opgenomen in beleid. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen significante aanvullende zekerheid geeft om beveiligingsrisico's verder te reduceren.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
5.1.2	Beoordeling van het informatiebeveiligingsbeleid: Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	CA-17	IS-1 IS-2	Controls aanwezig in assurance rapportage (SOC)	Ontbreken control in SOC geaccepteerd door werkgroep. Uit de control CA-17 in de assurance rapportage blijkt niet duidelijk of en hoe vaak het beveiligingsbeleid wordt gereviewd. Uit de aanvullend ontvangen FedRAMP-rapportage (geen assurance) is op te maken dat het beveiligingsbeleid jaarlijks gereviewd wordt. Dit is opgenomen onder AU-01/AU-02 in de FedRAMP-rapportage. Aangezien enkel ontbreekt hoe vaak het beleid wordt gereviewd en uit aanvullend ontvangen FedRAMP-rapportage is gebleken dat het beleid jaarlijks wordt gereviewd, heeft de werkgroep risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is.	
5.1.2.1	Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.	CA-17	IS-1 IS-2	Ontbreken control in SOC geaccepteerd door werkgroep. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance nodig is, ondanks dat het niet mogelijk is vast te stellen dat het informatiebeveiligingsbeleid periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen wordt beoordeeld en zo nodig wordt bijgesteld. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel aantonen van de specifieke bestuurs- en P&C-cycli in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	CA-17	IS-3	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
6.1.1.1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	CA-17	IS-3	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
6.1.1.2	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	CA-17	IS-3	Controls aanwezig in ISO control mapping/NIST raamwerk Relatie tot voorschriften en wetten is niet specifiek vermeld in de assurance rapportages. Hiervoor is wel aanvullende informatie (geen assurance) aangeleverd door Microsoft. Dit betreffen rapportages betreffende ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365 identificeert personen met informatiesysteembeveiligingsrollen en -verantwoordelijkheden. Het M365-beveiligingsbeleid richt zich op doel, reikwijdte, rollen, verantwoordelijkheden, nalevingsvereisten en vereiste coördinatie tussen de verschillende Microsoft-organisaties die een bepaald niveau van ondersteuning bieden voor de beveiliging van M365. M365-beveiligingsbeleid bevat regels en vereisten waaraan moet worden voldaan in de levering en werking van M365. M365-medewerkers en tijdelijk personeel zijn verantwoordelijk en verantwoordelijk voor de naleving van deze leidende principes in hun toegewezen rollen. Azure identificeert personen met informatiebeveiligingsrollen en -verantwoordelijkheden; en definieert en documenteert informatiebeveiligingsrollen en -verantwoordelijkheden gedurende de gehele levenscyclus van systeemontwikkeling. Daarnaast staat in de DPA (https://aka.ms.dpa): "(*...) Microsoft will Assurance aanwezig with all laws and regulations applicable to its providing the Products and Services, including security breach notification law and Data Protection Requirements(...)". Derhalve is uit de aangeleverde documentatie (geen assurance) op te maken dat de verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
6.1.1.3	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	CA-17	IS-3	Ontbreken control in SOC geaccepteerd door werkgroep. De werkgroep heeft risicogebaseerd aangegeven dat deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd heeft. Het wel kunnen aantonen van de rol en verantwoordelijkheden van de CISO in de overheidsmaatregel geeft geen aanvullende zekerheid betreffende de bovenliggende BIO-control.		
6.1.1.4	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	CA-17	IS-3	Ontbreken control in SOC geaccepteerd door werkgroep. De werkgroep heeft risicogebaseerd aangegeven dat deze overheidsmaatregel geen aanvullende assurance benodigd heeft. De werkgroep geeft aan dat het wel aantonen van de rol en verantwoordelijkheden van de CISO in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
6.1.2	Scheiding van taken: Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	CA-08 CA-33.a CA-33.b CA-35.a CA-35.b CA-39 CA-43 *CC6.3*	IS-3 *CC-6.3*	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	M365 - CUEC-01: De gebruikersorganisatie is verantwoordelijk voor het op de juiste manier autoriseren van gebruikers die toegang krijgen tot de bronnen en het bewaken van de voortdurende geschiktheid van toegang. M365 - CUEC-06: De gebruikersorganisatie is verantwoordelijk voor het beveiligen van de software en hardware die worden gebruikt om toegang te krijgen tot M365.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
6.1.2.1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	CA-08 CA-33.a CA-33.b CA-35.a CA-35.b CA-39 CA-43 *CC6.3*	IS-3 *CC-6.3*	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Zie 6.1.2
6.1.3	Contact met overheidsinstanties: Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.	CA-25	SOC2 - 18 SOC2 - 19	Ontbreken control in SOC geaccepteerd door werkgroep. Contacten met overheidsinstanties zijn niet expliciet opgenomen in assurance rapportages. Uit aanvullend ontvangen FedRAMP-rapportage (geen assurance) is op te maken dat het M365 SIR (Security Incident Response)-team incidenten rapporteert aan aangewezen autoriteiten (inclusief US-CERT, het United States Computer Emergency Readiness Team) in overeenstemming met NIST SP 800-61 zoals gedocumenteerd in het M365 SIR (Security Incident Response) Plan. Tevens is uit de FedRAMP-rapportage op te maken dat het Azure Security-team coördineert met de ISSO (Information System Security Officer) om de juiste overheidscontacten op de hoogte te stellen, inclusief (indien van toepassing) geautoriseerde functionarissen, overheidsklanteninstanties, US-CERT en anderen, van een incident, incidentupdates en oplossing. Dit is opgenomen onder IR-06 in de Azure FedRAMP-rapportage en IR-6 in de M365 FedRAMP-rapportage. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien uit bovenstaande blijkt dat passende contacten met relevante overheidsinstanties worden onderhouden.		
6.1.3.1	Er is door de organisatie uitgewerkt wie met welke (overheids)instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.	CA-25	SOC2 - 18 SOC2 - 19	Ontbreken control in SOC geaccepteerd door werkgroep. Uit assurance rapportages van Azure en M365 is niet op te maken of door Microsoft uitgewerkt is wie met welke (overheids)instanties en toezichthouders contact is ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn. Hiervoor is wel aanvullende informatie aangeleverd door Microsoft. Dit betreffen rapportages betreffende ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Microsoft werkt voor M365 samen met het Microsoft Trustworthy Computing Team om contacten te onderhouden met externe partijen zoals regelgevende instanties, serviceproviders en brancheorganisaties, zoals het United States Computer Emergency		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				Readiness Team (US-CERT) om ervoor te zorgen dat snel passende maatregelen kunnen worden genomen en advies kan worden ingewonnen wanneer vereist. M365 vertrouwt op de wereldwijde 'Criminal compliance'- en 'Corporate, External and Legal Affairs' (CELA)-teams van Microsoft voor contacten met wetshandhavingsinstanties. Rollen en verantwoordelijkheden voor het beheren en onderhouden van deze relaties zijn gedefinieerd. Betreffende Azure wordt gerapporteerd over beveiligingsincidenten aan aangewezen autoriteiten (inclusief US-CERT) zoals gedocumenteerd in het Microsoft Azure Incident Response Plan. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien uit aanvullende informatie voldoende blijkt dat de organisatie heeft uitgewerkt wie met welke instanties en toezichthouders contact heeft.		
6.1.3.2	Het contactoverzicht wordt jaarlijks geactualiseerd.	CA-25	SOC2 - 18 SOC2 - 19	Ontbreken control in SOC geaccepteerd door werkgroep. Uit assurance rapportages van Azure en M365 niet op te maken of het contractoverzicht jaarlijks wordt geactualiseerd. Op basis van de rapportages betreffende ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure is niet op te maken of het contactoverzicht jaarlijks wordt geactualiseerd. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het aantonen van jaarlijkse actualiseren van het contactoverzicht geen aanvullende zekerheid geeft ten opzichte van de control.		
6.1.4	(Vervallen)					
6.1.5	Informatiebeveiliging in projectbeheer: Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.	n.v.t	n.v.t	Controls aanwezig in FedRAMP-raamwerk Uit de assurance rapportages is niet duidelijk of informatiebeveiliging aan de orde komt in projectbeheer, ongeacht het soort project. Uit aanvullende ontvangen FEDRAMP-rapportages (geen assurance) is op te maken dat informatiebeveiliging wordt meegenomen in business process planning, waaronder ook in projecten. Dit is opgenomen onder SA-02 in de Azure-FedRAMP-rapportage en SA-2 in de M365-FedRAMP rapportage.		
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
6.2.1	Beleid voor mobiele apparatuur: Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	n.v.t	CCM - 1	Controls aanwezig in FedRAMP-raamwerk Uit assurance rapportage van M365 niet op te maken of beleid en ondersteunende maatregelen voor mobiele apparatuur vastgesteld zijn. Uit aanvullende ontvangen FEDRAMP-rapportage (geen assurance) is op te maken dat binnen de M365 boundary geen mobiele apparatuur aanwezig is. Dit is opgenomen onder AC-19 in de M365 FedRAMP rapportage.	Controls aanwezig in assurance rapportage (SOC)	
6.2.1.1	Mobiele apparatuur is zo ingericht dat bedrijfsinformatie niet onbewust wordt opgeslagen ('zero footprint'). Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die gegevens. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn.	n.v.t	CCM - 1	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk vast te stellen dat mobiele apparatuur zo is ingericht dat bedrijfsinformatie niet onbewust wordt opgeslagen ('zero footprint') of dat als zero footprint (nog) niet realiseerbaar is, een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid biedt om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die gegevens plaatsvindt. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
6.2.1.2	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: a) In bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde. b) Het device maakt deel uit van patchmanagement en hardening. c) Er wordt gebruik gemaakt van Mobile	n.v.t.	CCM - 1	Controls aanwezig in ISO-control mapping/NIST raamwerk Uit assurance rapportages van Azure en M365 is niet op te maken of de aspecten zoals in de overheidsmaatregelen beschreven zijn geïmplementeerd. Daarnaast is voor M365 geen specifieke control in de assurance rapportage opgenomen over inzet van mobiele apparatuur, enkel een beschrijving van de control (For Microsoft employees and other internal users, access to M365 applications and supporting services infrastructure through mobile devices is restricted and managed by the Microsoft Datacenters group).		Algemeen - CUEC: De gebruikersorganisatie is (bij de inzet van mobiele apparatuur) verantwoordelijk voor het implementeren van de aspecten zoals genoemd in de overheidsmaatregel.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
	Device Management MDM of van Mobile Application Management (MAM)-oplossingen. d) Gebruikers tekenen een gebruikersovereenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen. Deze verklaring heeft betrekking op alle mobiele apparatuur die de medewerker zakelijk gebruikt. e) Periodiek wordt getoetst of de punten in lid a), b) en c) worden nageleefd.			Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreffen rapportages over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Microsoft heeft een beleid en ondersteunende beveiligingsmaatregelen om risico's te beheersen die worden veroorzaakt door het gebruik van mobiele apparaten. Ongeautoriseerde mobiele computerapparaten zijn niet toegestaan in, of direct aangesloten op, een M365-productieomgeving. Microsoft-personeel en tijdelijk personeel moeten passende beveiligingspraktijken toepassen en volgen bij het gebruik van mobiele computerapparatuur om te beschermen tegen de risico's van het gebruik van mobiele apparatuur. Dergelijke risico's hebben betrekking op de mobiele aard van deze apparaten, en de beveiligingspraktijken die door Microsoft zijn toegepast om deze risico's te beperken, kunnen onder meer omvatten, maar zijn niet beperkt tot, fysieke beveiliging van mobiele apparaten, toegangscontrole, cryptografische vereisten, virusbeveiliging en/of het controleren van locaties van waaruit de apparaten verbinding kunnen maken. Apparaten voor mobiel computergebruik en gegevensregistratie zijn onder meer PDA's, draagbare harde schijven, laptops, flashdrives, andere opneembare media, enz. Microsoft controleert op ongeoorloofd gebruik van mobiele apparaten in de M365-omgeving en voert dienovereenkomstig onderzoeken uit. M365-middelen worden opgesloten in kooien in Microsoft-faciliteiten die toegangscontrole hebben. Terwijl M365-technici fysieke toegang hebben tot de servers in de kooien, hebben ze niet de logische toegang tot de servers die nodig zouden zijn om gebruik te maken van draagbare media. Azure geeft geen verbinding via mobiele apparaten met Azure en staat deze toegang ook niet toe. Bovendien bevatten systemen binnen Azure geen draadloze netwerkmogelijkheden. Alle netwerkconnectiviteit voor de Azure-omgeving is via bekabeling en activa hebben geen interne ingebouwde draadloze technologie. Draadloze toegang is niet toegestaan binnen de Azure-omgeving. Daarnaast mogen apparaten voor mobiele computers en gegevensregistratie niet worden gebruikt in een van de productieomgevingen van Microsoft zonder voorafgaande goedkeuring door het Datacenter Management Team via een toegangsverzoek. Azure bewaakt al het ongeoorloofd gebruik van mobiele apparaten in de Azure-omgeving en voert dienovereenkomstig onderzoeken uit. Azure gebruikt een groen/rood stickersysteem om geautoriseerde apparaten te identificeren. Bewaking van ongeautoriseerde verbindingen van mobiele apparaten met servers wordt uitgevoerd door beveiligingsfunctionarissen die observeren dat alle mobiele apparaten die op servers worden gebruikt, overeenkomstige vermeldingen in het DCAT-systeem moeten hebben, dat de autorisatie voor een persoon vastlegt om een mobiel apparaat naar het datacenter te brengen. Uit bovenstaande is niet expliciet op te maken of punten A t/m E worden nageleefd.		Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het beoordelen van openbare Azure-beveiligings- en patchupdates. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het toepassen van patches indien zij niet is aangemeld voor automatische upgrades.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
6.2.2	Telewerken: Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.	CA-36 CA-40 CA-41	OA - 8	Controls aanwezig in FedRAMP-raamwerk Uit de assurance rapportages is niet duidelijk of beleid en beveiligingsmaatregelen geïmplementeerd zijn ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd. Uit aanvullende ontvangen FEDRAMP-rapportage (geen assurance) is op te maken dat indien een gebruiker niet op een fysieke Microsoft-locatie aanwezig is, toegang op afstand (hierna: remote access) vereist dat gebruik wordt gemaakt van een Microsoft VPN-verbinding gebruikmakend van door Microsoft uitgegeven smartcard-certificaten en authenticatie met pincode in aanvulling op de reguliere toegangsbeveiligingsmaatregelen. Dit is opgenomen onder AC-17 in de Azure FedRAMP-rapportage. Tevens is uit ontvangen FEDRAMP-rapportage (geen assurance) op te maken dat beheeractiviteiten voor Microsoft altijd via remote access uitgevoerd worden, aangezien de teams geen toegang hebben tot de datacenters. Hierbij wordt gebruik gemaakt van Terminal Services Gateways (TSGs) met twee-factor authenticatie en Secure Access Workstations (SAWs). Dit is opgenomen onder AC-17 in de M365 FedRAMP-rapportage.		M365 - CUEC-01: De gebruikersorganisatie is verantwoordelijk voor het op de juiste manier autoriseren van gebruikers die toegang krijgen tot de bronnen en het bewaken van de voortdurende geschiktheid van toegang. M365 - CUEC-02: De gebruiker-organisatie is verantwoordelijk voor het inrichten van controles omtrent het gebruik van systeem-ID's en wachtwoorden. M365 - CUEC-03: De gebruikersorganisatie is verantwoordelijk voor het beheer van het wachtwoord-authenticatiemechanisme van hun gebruikers. M365 - CUEC-06: De gebruikersorganisatie is verantwoordelijk voor het beveiligen van de software en hardware die worden gebruikt om toegang te krijgen tot M365. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
						voor het implementeren van logische toegangscontroles om redelijke zekerheid te bieden dat ongeautoriseerde toegang tot belangrijke systemen wordt beperkt.
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
7.1.1	Screening: Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.	CA-08	SOC2 - 12	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor de naleving van toepasselijke wet-/regelgeving.
7.1.1.1	Elke organisatie heeft een vastgesteld screeningsbeleid. Bij indiensttreding en bij functiewijziging kan een Verklaring Omtrent het Gedrag (VOG) gevraagd worden.	CA-08	SOC2 - 12	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
7.1.2	Arbeidsvoorwaarden: De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	CA-17 ELC-08	SOC2 - 13	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
7.1.2.1	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.	CA-17 ELC-08	SOC2 - 13	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
7.2.1	Directieverantwoordelijkheden: De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	ELC-08	SOC2 - 13	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
7.2.1.1	Er is aansluiting bij een klokkenluidersregeling, zodat iedereen in staat is om anoniem en veilig beveiligingsissues te kunnen melden.	ELC-08	SOC2 - 13	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging: Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	CA-07	IS - 4 ELC - 2	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
7.2.2.1	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen	CA-07	IS - 4 ELC - 2	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
7.2.2.2	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen- en diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.	CA-07	IS - 4 ELC - 2	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om uit assurance rapportages op te maken binnen welke termijn trainingen gevolgd moeten worden. Daarnaast is een training I-bewustzijn niet expliciet genoemd in de assurance rapportages. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
7.2.2.3	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij haar medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.	CA-07	IS - 4 ELC - 2	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om uit assurance rapportages op te maken dat dit wordt benadruk bij aanstelling, overplaatsing, werkoverleggen en personeelsgesprekken. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
7.2.3	Disciplinaire procedure: Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	ELC-08	SOC2 - 11	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband: Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht.	ELC-08 CA-43	*HRS-01* SOC2 - 13	Ontbreken control in SOC geaccepteerd door werkgroep. Uit de assurance rapportages is niet duidelijk of verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht. Uit aanvullende ontvangen FEDRAMP-rapportage (geen assurance) is op te maken dat een exit survey wordt gestuurd naar Azure-personeel dat overstapt naar een concurrent. In deze exit survey wordt tevens de non-disclosure behandeld. Deze survey wordt niet uitgevoerd indien het personeel niet naar een concurrent gaat. Dit is opgenomen onder PS-04 in de Azure FedRAMP-rapportage. Tevens is uit aanvullende ontvangen FEDRAMP-rapportage (geen assurance) op te maken dat een exitinterview plaatsvindt met M365 personeel dat vrijwillig uit dienst gaat. In dit exitinterview wordt tevens de non-disclosure agreement behandeld. Exitinterviews vinden niet plaats in geval van gedwongen uitdiensttreding. Dit is opgenomen onder PS-4 in de M365 FedRAMP-rapportage. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien uit de assurance rapportage blijkt dat deze verantwoordelijkheden bij indiensttreding worden behandeld.		
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
8.1.1	Inventariseren van bedrijfsmiddelen: Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.	CA-17	SOC2 - 1	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
8.1.2	Eigendom van bedrijfsmiddelen: Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.	CA-17	SOC2 -1 SOC2 - 2	Controls aanwezig in FedRAMP-raamwerk Uit de assurance rapportages is niet op te maken dat alle bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden een eigenaar behoren te hebben. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is op te maken dat de inventarisinformatie ook het serviceteam betreft dat verantwoordelijk is voor ieder component van het informatiesysteem. Elk serviceteam wijst een of meer personen of rollen aan die verantwoordelijk zijn voor het beheer van de onderdelen van dat team als aangewezen eigenaren van de bedrijfsmiddelen. Dit is opgenomen onder CM-8 in de M365-FedRAMP-rapportage. Tevens is uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) op te maken dat eigenaren van bedrijfsmiddelen verplicht zijn om hun bedrijfsmiddelen te classificeren, en dat geen bedrijfsmiddelen zijn vrijgesteld van deze eis. Hieruit is op te maken dat ieder bedrijfsmiddel een eigenaar heeft. Dit is opgenomen onder MP-07 in de Azure FedRAMP-rapportage.		Algemeen - CUEC: Voor de bedrijfsmiddelen waarmee Microsoft-diensten worden gebruikt, dienen gebruikersorganisaties een inventarisoverzicht bij te houden, inclusief een eigenaar per bedrijfsmiddel.
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen: Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	ELC-08	SOC2 - 13	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
8.1.3.1	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.	ELC-08	SOC2 - 13	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
8.1.3.2	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel in het contract vastgelegd overeenkomstig de huisregels of gedragsregels.	ELC-08	SOC2 - 13	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
8.1.4	Teruggeven van bedrijfsmiddelen: Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven.	ELC-08	*HRS-01* SOC2 - 13	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
8.2.1	Classificatie van informatie: Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	CA-17 CA-66	SOC2 - 1 SOC2 - 2	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor de naleving van toepasselijke wet-/regelgeving.
8.2.1.1	De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.	CA-17 CA-66	SOC2 - 1 SOC2 - 2	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
8.2.2	Informatie labelen: Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	n.v.t.	SOC2 - 1 SOC2 - 2 *DSI-04*	Controls aanwezig in FedRAMP-raamwerk In de assurance rapportage is het labelen van data niet expliciet opgenomen. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is op te maken dat de Microsoft Enterprise Online Services Data Taxonomy (oftewel Asset Classification Standard) en M365 Data Handling Standard passende behandelings- en beschermingsprocedures van data definiëren op basis van hun classificatie. Hieruit is op te maken dat informatie gelabeld wordt. Dit is opgenomen onder MP-01 in de M365 FedRAMP-rapportage.	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
8.2.3	Behandelen van bedrijfsmiddelen: Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	CA-08 CA-32 CA-33.a CA-33.b CA-34 CA-35.a CA-35.b CA-36 CA-37 CA-39 CA-40 CA-41 CA-56 CA-57 CA-58 CA-59 CA-60 CA-61 CA-64 CA-65 *CC6.1*	SOC2 - 1 SOC2 - 2 SOC2 - 3 *DSI-04*	Controls aanwezig in FedRAMP-raamwerk In de assurance rapportage is het behandelen van bedrijfsmiddelen niet expliciet opgenomen. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is op te maken dat de Microsoft Enterprise Online Services Data Taxonomy (oftewel Asset Classification Standard) en M365 Data Handling Standard passende behandelings- en beschermingsprocedures van data definiëren op basis van hun classificatie. Hieruit is op te maken dat procedures voor het behandelen van bedrijfsmiddelen worden geïmplementeerd. Dit is opgenomen onder MP-01 in de M365 FedRAMP-rapportage.	Controls aanwezig in assurance rapportage (SOC)	M365 - CUEC-01: De gebruikersorganisatie is verantwoordelijk voor het op de juiste manier autoriseren van gebruikers die toegang krijgen tot de bronnen en het bewaken van de voortdurende geschiktheid van toegang. M365 - CUEC-04: De gebruikersorganisatie is verantwoordelijk voor het afdwingen van het gewenste versleutelingsniveau voor netwerk-sessies. M365 - CUEC-06: De gebruikersorganisatie is verantwoordelijk voor het beveiligen van de software en hardware die worden gebruikt om toegang te krijgen tot M365.
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
8.3.1	Beheer van verwijderbare media: Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	*CC6.4*	SOC2 - 3 DS - 10	Ontbreken control in SOC geaccepteerd door werkgroep. Microsoft steunt voor deze control op Azure, waardoor enkel het Azure assurance rapport van toepassing is.	Controls aanwezig in assurance rapportage (SOC)	
8.3.1.1	Er is een verwijderinstructie waarin is opgenomen dat van herbruikbare media die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd (ISO27002 – implementatierichtlijn 8.3.1.a).	*CC6.4*	SOC2 - 3 DS - 10	Ontbreken control in SOC geaccepteerd door werkgroep. Voor M365 wordt gesteund op Azure. Uit de assurance rapportage van Azure is niet op te maken of een verwijderinstructie aanwezig is waarin is opgenomen dat van herbruikbare media die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd (ISO27002 – implementatierichtlijn 8.3.1.a). Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreffen rapportages (geen assurance) voor ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Microsoft ontwikkelt, documenteert en verspreidt onder door de organisatie gedefinieerde medewerkers of rollen procedures om de implementatie van het mediabeschermingsbeleid en bijbehorende mediabeschermingsmaatregelen te vergemakkelijken. Microsoft maakt geen gebruik van verwisselbare media binnen de M365 -productieomgeving. Eigenaren van bedrijfsmiddelen zijn verplicht om hun bedrijfsmiddelen een bedrijfsmiddelenclassificatie toe te kennen en geen bedrijfsmiddelen zijn vrijgesteld van deze vereiste. In de Azure-datacenteromgeving verwijzen naar servers, netwerkapparaten en magnetische banden. In de datacenters wordt geen gebruik gemaakt van niet-digitale media. Azure gebruikt gegevensverwijderingseenheden en -processen om gegevens op te schonen in overeenstemming met NIST SP 800-88 revisie 1, die in overeenstemming zijn met de Azure-bedrijfsmiddelenclassificatie van het bedrijfsmiddel. Voor bedrijfsmiddelen die moeten worden vernietigd, maakt Azure gebruik van services voor het vernietigen van bedrijfsmiddelen op locatie. In Azure-datacenters worden de digitale media van Azure opgeschoond met behulp van door Azure goedgekeurde hulpprogramma's en in overeenstemming met NIST SP 800-88 revisie 1 voordat ze opnieuw worden gebruikt. Uit bovenstaande is niet op te maken of een verwijderinstructie aanwezig is waarin wordt ingegaan op het onherstelbaar verwijderen van de inhoud van herbruikbare media. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien het aantonen van deze maatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
8.3.2	Verwijderen van media: Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	*CC6.4*	SOC2 - 3 DS - 12	Ontbreken control in SOC geaccepteerd door werkgroep. Microsoft steunt voor deze control op Azure, waardoor enkel het Azure assurance rapport van toepassing is.	Controls aanwezig in assurance rapportage (SOC)	Algemeen - CUEC: De gebruikersorganisatie is verantwoordelijk voor het eigen gebruik van verwijderbare media.
8.3.2.1	Media die vertrouwelijke informatie bevatten, zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden.	*CC6.4*	SOC2 - 3 DS - 12	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Zie 8.3.2
8.3.2.2	Verwijdering vindt plaats op een veilige manier, bijvoorbeeld door verbranding of versnippering. Verwijdering van alleen gegevens is ook mogelijk door het wissen van de gegevens voordat de media worden gebruikt voor een andere toepassing in de organisatie (ISO 27002 – implementatierichtlijn 8.3.2.a).	*CC6.4*	SOC2 - 3 DS - 12	Ontbreken control in SOC geaccepteerd door werkgroep. In M365 assurance rapportage wordt gesteund op Azure. Uit assurance rapportages van Azure en M365 is niet op te maken op welke wijze verwijdering plaatsvindt. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreffen rapportages over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Microsoft verwijdert media veilig als ze niet langer nodig zijn, met behulp van formele procedures. Microsoft reinigt media voorafgaand aan verwijdering, vrijgave buiten organisatorische controle of vrijgave voor hergebruik in overeenstemming met toepasselijke federale en organisatorische normen en beleid. Microsoft blijft verantwoordelijk voor bedrijfsmiddelen die het datacenter verlaten door het gebruik van NIST SP 800-88 consistente processen voor opschonen/opruimen, vernietiging van bedrijfsmiddelen, versleuteling, nauwkeurige inventarisatie, tracking en bescherming van de bewakingsketen tijdens transport. Azure: Digitale media in Azure-datacenters die de Azure-omgeving hosten, bestaan uit servers, netwerkapparaten en fysieke harde schijven. Azure-datacenters gebruiken geen niet-digitale media. Digitale media binnen Azure mogen niet vanaf de Azure-locatie worden getransporteerd, tenzij deze worden vernietigd. Bedrijfsmiddelen die moeten worden vernietigd, worden opgeslagen in afgesloten opslagbakken. Op het moment van vernietiging en onder toezicht van cameratoezicht worden Azure digitale media uit de vergrendelde opslagbak verwijderd en gescand om het serienummer van het te vernietigen bedrijfsmiddel vast te leggen. Het bedrijfsmiddel wordt versnipperd terwijl het wordt gecontroleerd door goedgekeurd personeel. De vernietigingsverkoper geeft een certificaat van vernietiging af voor de bedrijfsmiddelen die werden vernietigd.		Zie 8.3.2

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				Uit bovenstaande is op te maken dat de methoden die voldoen aan de NIST SP 800-88 worden gebruikt voor verwijderen van data. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien uit de assurance rapportage reeds blijkt dat data is versleuteld en wordt vernietigd.		
8.3.2.3	Voor het wissen van alle data op het medium, wordt de data onherstelbaar verwijderd, bijvoorbeeld door minimaal twee keer te overschrijven met vaste data en één keer met random data. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is.	*CC6.4*	SOC2 - 3 DS - 12	Ontbreken control in SOC geaccepteerd door werkgroep. In M365 assurance rapportage wordt gesteund op Azure. Uit assurance rapportages van Azure en M365 niet op te maken of de data onherstelbaar verwijderd wordt, en of dit wordt gecontroleerd. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Microsoft verwijdert media veilig wanneer ze niet langer nodig zijn, met behulp van formele procedures. Microsoft reinigt media voorafgaand aan verwijdering, vrijgave buiten organisatorische controle of vrijgave voor hergebruik in overeenstemming met toepasselijke federale en organisatorische normen en beleid. Microsoft blijft verantwoordelijk voor bedrijfsmiddelen die het datacenter verlaten door het gebruik van NIST SP 800-88 consistente processen voor opschonen/opruimen, vernietiging van bedrijfsmiddelen, versleuteling, nauwkeurige inventarisatie, tracking en bescherming van de bewakingsketen tijdens transport. Azure gebruikt gegevensverwijderingseenheden en -processen om gegevens op te schonen in overeenstemming met NIST SP 800-88 revisie 1 voordat ze opnieuw worden gebruikt. Elke honderdtachtig (180) dagen test het Cyber Defense Operations Center (CDOC) de Azure-eenheden voor het wissen van gegevens en het proces voor het wissen. In de test verifieert Cloud Operations + Innovation Engineering (CO + IE) dat de beoogde opschoning wordt bereikt door een forensische analyse van geteste harde schijven om te bevestigen dat de gegevens zijn opgeschoond door de gegevenswissers. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien uit de assurance rapportage reeds blijkt dat data is versleuteld en het aantonen van deze maatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		Zie 8.3.2

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
8.3.3	Media fysiek overdragen: Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	*CC6.4*	SOC2 - 1 CCM - 1	Ontbreken control in SOC geaccepteerd door werkgroep. In M365 assurance rapportage wordt gesteund op Azure. Aanvullende informatie is aangeleverd door Microsoft. Dit betreft rapportages over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Microsoft gebruikt drie methoden om media tijdens transport buiten het datacenter te beveiligen: 1) Beveiligd transport, 2) encryptie, and 3) reinigen, zuiveren of vernietigen. Microsoft heeft een contract gesloten met verschillende goedgekeurde leveranciers om veilige verzendservices te bieden. Azure handhaaft verantwoordelijkheid voor bedrijfsmiddelen die het datacenter verlaten in overeenstemming met NIST SP 800-88: consistent opschonen/opschonen, vernietiging van bedrijfsmiddelen, encryptie, nauwkeurig inventarisatie, tracking en bescherming van de chain of custody tijdens transport. De werkgroep heeft risicogebaseerd aangegeven dat voor deze control geen aanvullende verduidelijking of assurance benodigd is aangezien Microsoft wel over controls beschikt die er zorg voor dragen dat data beveiligd wordt getransporteerd, gereinigd of vernietigd.		
8.3.3.1	Er is een vastgestelde procedure voor het fysiek transport van media.	Zie Azure	SOC2 - 3	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
8.3.3.2	Het gebruik van koeriers of transporteurs voor transport van op BBN2 of hoger geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.	*CC6.4*	SOC2 - 1 CCM - 1	Ontbreken control in SOC geaccepteerd door werkgroep. In M365 assurance rapportage wordt gesteund op Azure. Aanvullende informatie is aangeleverd door Microsoft. Dit betreft rapportages over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Microsoft gebruikt drie methoden om media tijdens transport buiten het datacenter te beveiligen: 1) Beveiligd transport, 2) encryptie, and 3) reinigen, zuiveren of vernietigen. Microsoft heeft een contract gesloten met verschillende goedgekeurde leveranciers om veilige verzendservices te bieden. Azure heeft een contract gesloten met verschillende goedgekeurde leveranciers om veilige verzendservices te bieden. Vereisten voor het transport van bedrijfsmiddelen worden gedefinieerd op basis van hun bedrijfsmiddelenclassificatie en gegevensclassificatie. Uit bovenstaande is niet op te maken of bij het gebruik van koeriers voor transport van op BBN2 of hoger geclassificeerde informatie wordt voldaan aan vooraf opgestelde betrouwbaarheidseisen. Per interview met Microsoft hebben wij vernomen dat voor het fysiek overdragen van media geen onderscheid wordt gemaakt in klantinformatie, alle informatie/data van klanten (customer data) wordt door Microsoft geclassificeerd als 'high business impact'.		Algemeen - CUEC: De gebruikersorganisatie is verantwoordelijk voor de classificatie van informatie naar BBN-standaarden en het opstellen van betrouwbaarheids-eisen.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien uit de assurance rapportage reeds blijkt dat data is versleuteld en het aantonen van deze maatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
9.1.1	Beleid voor toegangsbeveiliging: Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	CA-17	IS - 1 IS - 2	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
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.	CA-32 CA-33.a CA-33.b CA-35.a CA-35.b CA-36 CA-39 CA-56 CA-57	OA - 9 OA - 10 OA - 13 OA - 14	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	M365 - CUEC-01: De gebruikersorganisatie is verantwoordelijk voor het op de juiste manier autoriseren van gebruikers die toegang krijgen tot de bronnen en het bewaken van de voortdurende geschiktheid van toegang. M365 - CUEC-06: De gebruikersorganisatie is verantwoordelijk voor het beveiligen van de software en hardware die worden gebruikt om toegang te krijgen tot M365.
9.1.2.1	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.	CA-32 CA-33.a CA-33.b CA-35.a CA-35.b CA-36 CA-39 CA-56 CA-57	OA - 9 OA - 10 OA - 13 OA - 15	Controls aanwezig in ISO control mapping / NIST raamwerk In assurance rapportages wordt niet gesproken over geauthentiseerde apparatuur. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Microsoft heeft een beleid en ondersteunende beveiligingsmaatregelen aangenomen om de risico's te beheersen die worden veroorzaakt door het gebruik van mobiele apparaten. Ongeautoriseerde mobiele computerapparaten zijn niet toegestaan in, of direct aangesloten op, een M365-productieomgeving. Medewerkers van het M365-team krijgen alleen toegang tot netwerken en netwerkservices waarvoor ze specifiek zijn geautoriseerd. Standaard heeft niemand toegang tot klantinhoud zonder autorisatie. Azure identificeert en verifieert op unieke wijze alle apparaten binnen de Microsoft Azure-accreditatiegrens voordat een netwerkverbinding tot stand wordt gebracht.		Zie 9.1.2

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
9.1.2.2	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.	CA-32 CA-33.a CA-33.b CA-35.a CA-35.b CA-36 CA-39 CA-56 CA-57	OA - 9 OA - 10 OA - 13 OA - 16	Controls aanwezig in ISO control mapping / NIST raamwerk In assurance rapportages wordt niet gesproken over het gebruik van eigen of ongeauthenticeerde apparatuur. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Microsoft heeft een beleid en ondersteunende beveiligingsmaatregelen aangenomen om risico's te beheersen die worden veroorzaakt door het gebruik van mobiele apparaten. Ongeautoriseerde mobiele computerapparaten zijn niet toegestaan in, of direct aangesloten op, een M365-productieomgeving. Microsoft-personeel en tijdelijk personeel moeten passende beveiligingspraktijken toepassen en volgen bij het gebruik van mobiele computerapparatuur om te beschermen tegen de risico's van het gebruik van mobiele apparatuur. Azure identificeert en authentiseert op unieke wijze alle apparaten (zowel fysiek als virtueel) binnen de Microsoft Azure-accreditatiegrens voordat een netwerkverbinding tot stand wordt gebracht. Per interview met Microsoft is tevens vernomen dat geen Bring Your Own Device van toepassing is voor M365 en Azure.		Zie 9.1.2

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
9.2.1	Registratie en afmelden van gebruikers: Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	CA-08 CA-32 CA-33.a CA-33.b CA-34 CA-35.a CA-35.b CA-43	OA - 1 OA - 2 OA - 3 OA - 5 OA - 6 OA -7	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	M365 - CUEC-01: De gebruikersorganisatie is verantwoordelijk voor het op de juiste manier autoriseren van gebruikers die toegang krijgen tot de bronnen en het bewaken van de voortdurende geschiktheid van toegang. M365 - CUEC-06: De gebruikersorganisatie is verantwoordelijk voor het beveiligen van de software en hardware die worden gebruikt om toegang te krijgen tot M365. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het uitschakelen/ verwijderen van accounttoegang tot hun Azure-services bij wijziging of beëindiging van de rol van werknemers en contractanten. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het inrichten van passende controles over het gebruik van

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
						hun Microsoft-accounts en wachtwoorden.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
9.2.1.1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	CA-08 CA-32 CA-33.a CA-33.b CA-34 CA-35.a CA-35.b CA-43	OA - 1 OA - 2 OA - 3 OA - 5 OA - 6 OA -7	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Zie 9.2.1
9.2.1.2	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	CA-08 CA-32 CA-33.a CA-33.b CA-34 CA-35.a CA-35.b CA-43	OA - 1 OA - 2 OA - 3 OA - 5 OA - 6 OA -7	Controls aanwezig in FedRAMP-raamwerk Voor M365 is een control aanwezig omtrent toegang tot 'shared accounts'. Het is echter Het is niet mogelijk om vast te stellen op basis van assurance rapportages of het gebruik van dergelijke accounts wordt gemotiveerd en vastgelegd door de proceseigenaar. Uit aanvullend ontvangen FedRAMP-rapportage voor M365 is op te maken dat M365 het gebruik van gedeelde/groepsserviceteamaccounts niet toestaat, tenzij de vereiste om gebruikersactiviteit op unieke wijze aan het account toe te kennen is geïmplementeerd; uitzonderingen kunnen per geval worden goedgekeurd. Tevens is uit aanvullend ontvangen M365 - Audited Controls NIST 800_53A Rev 4 (2016) op te maken dat M365 het gebruik van gedeelde/groepsgebruikersaccounts niet toestaat.	Controls aanwezig in ISO control mapping / NIST raamwerk Voor Azure is geen control aanwezig omtrent groepsaccounts. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over het NIST-framework (2021) voor Azure. Azure: Groepsaccounts of gedeelde accounts worden niet gebruikt binnen Azure, tenzij dit nodig is, bijvoorbeeld indien het lokale account of de lokale accounts niet kunnen worden verwijderd of uitgeschakeld, of wanneer dit nodig is voor noodtoegang. Voor accounts die worden bijgehouden als goedgekeurde uitzonderingen, worden de inloggegevens voor deze accounts opgeslagen in een goedgekeurd geheimbeheerarchief, dat de toegang tot geheimen volgt en bewaakt en ervoor zorgt dat het gebruik van groeps- of gedeelde accounts op unieke wijze kan worden toegeschreven aan de gebruiker die er toegang toe heeft door de geheime opslaglogboeken te koppelen aan het groeps- of gedeelde accountgebruik. Als een gebruiker toegang krijgt tot de inloggegevens in het geheime beheerarchief, wordt die gebruiker uniek	Zie 9.2.1

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
					geïdentificeerd, waardoor onweerlegbaarheid wordt gegarandeerd en gebruikersactiviteit wordt toegeschreven aan het gedeelde account.	
9.2.2	Gebruikers toegang verlenen: Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	CA-08 CA-32 CA-33.a CA-33.b CA-35.a CA-35.b CA-43	OA - 1 OA - 2 OA - 3 OA - 5 OA - 6 OA -7	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
9.2.2.1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	CA-08 CA-32 CA-33.a CA-33.b CA-35.a CA-35.b CA-43	OA - 1 OA - 2 OA - 3 OA - 5 OA - 6 OA -7	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
9.2.2.2	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	CA-08 CA-32 CA-33.a CA-33.b CA-35.a CA-35.b CA-43	OA - 1 OA - 2 OA - 3 OA - 5 OA - 6 OA -7	Controls aanwezig in ISO control mapping/NIST raamwerk Het is niet mogelijk om op te maken of (en welke) risicoafwegingen zijn gemaakt bij het toepassen van functiescheiding. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365 scheidt taken en verantwoordelijkheidsgebieden om de kans op ongeoorloofd gebruik, onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. M365-teams hebben rollen gedefinieerd als onderdeel van een uitgebreid, op rollen gebaseerd mechanisme voor toegangscontrole. Bovendien heeft elk M365-team rolparen geïdentificeerd die, indien toegewezen aan één persoon, kwaadaardige activiteiten mogelijk zouden maken zonder samenspanning. Als dergelijke rollenparen bestaan, mag geen enkel individu tot beide rollen behoren. Zo kunnen personen in elke rol met de mogelijkheid om		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				toegangsverzoeken goed te keuren, in heel M365 hun eigen toegangsverzoeken niet goedkeuren. Azure behandelt het toegangscontrolebeleid als onderdeel van het Microsoft-beveiligingsbeleid, waarvan er twee sets zijn: het Microsoft Security Policy (MSP) dat van toepassing is op al het personeel, en het Microsoft Security Program Policy (MSPP), dat van toepassing is op alle personeel dat verantwoordelijk is voor de beveiliging. De Microsoft Information Risk Management Council (IRMC) is het bestuursorgaan met beoordelings- en goedkeuringsverantwoordelijkheid voor de MSP en MSPP. Binnen Azure is de MSPP specifiek van toepassing op al het personeel dat betrokken is bij het ontwerpen, bouwen en exploiteren van Azure en op alle informatie en processen die worden gebruikt bij het uitvoeren van Microsoft-activiteiten. Alle Azure-medewerkers zijn verantwoordelijk en verantwoordelijk voor de naleving van deze leidende principes binnen hun toegewezen rollen. De policy gaat in op zowel toegangscontrole als functiescheiding. Daarnaast is scheiding van taken opgenomen in de Azure Access Control Standard Operating Procedures (SOP).		
9.2.2.3	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	CA-08 CA-32 CA-33.a CA-33.b CA-35.a CA-35.b CA-43	OA - 1 OA - 2 OA - 3 OA - 5 OA - 6 OA -7	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om op te maken of een actueel mandaatregister aanwezig is of functieprofielen aanwezig zijn waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Standaard heeft niemand toegang tot klantinhoud zonder autorisatie. Wanneer zich een probleem voordoet of een klant een serviceticket aanvraagt, moet een M365 on-call engineer (OCE) een speciale tool gebruiken om verhoogde bevoegdheden aan te vragen en te verkrijgen om het systeem binnen te komen en het probleem op te lossen. De tool bevindt zich tussen de OCE en de gegevens van de klant en controleert de reikwijdte van hun machtigingen voor het uitvoeren van bepaalde activiteiten. De tool keurt het verzoek goed of af en verleent, indien goedgekeurd, pas toegang nadat ook de goedkeuring van het management is verkregen. Azure: Alle accountgoedkeuringen voor Azure verlopen via OneIdentity. Alle beveiligingsgroepen hebben een geïdentificeerde primaire en secundaire eigenaar. Wanneer een gebruiker een verzoek indient, ontvangen deze goedkeurders een melding om goed te keuren of af te wijzen. Uit bovenstaande is op te maken dat de 'access approver role' onder andere kan liggen bij management en/of de eigenaren van de beveiligingsgroepen. Hieruit is echter niet op te maken of een actueel mandaatregister of functieprofielen aanwezig zijn waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien uit de aanvullende informatie reeds voldoende uiteengezet wordt op welke manier en door welke personen toegang wordt verleend en het aantonen van deze maatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
9.2.3	Beheren van speciale toegangsrechten: Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	CA-33.b CA-35.a CA-35.b	OA - 1 OA - 5	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het implementeren van de juiste authenticatiemechanismen en voor het alleen verlenen van beheerderstoegang aan de juiste personen om de integriteit van hun AAD-tenant te behouden. Azure - CUEC: Een gebruikersorganisatie die AAD-services gebruikt, is verantwoordelijk voor het implementeren van geschikte authenticatiemechanismen en het beperken van beheerderstoegang tot de juiste personen om de integriteit van hun SaaS-applicaties te behouden.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
9.2.3.1	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	CA-33.b CA-35.a CA-35.b	OA - 1 OA - 5	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
9.2.4	Beheer van geheime authenticatie-informatie van gebruikers: Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	CA-34	OA - 4	Controls aanwezig in FedRAMP-raamwerk In de assurance rapportage is het toewijzen van de authenticatie-informatie niet expliciet opgenomen. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is op te maken dat YubiKeys worden toegewezen door het M365 Security Team en dat (initiële) serviceteam domein-wachtwoorden automatisch worden gedistribueerd door account management tools. Dit is opgenomen onder IA-5 in de M365 FedRAMP-rapportage.	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het implementeren van de juiste authenticatiemechanismen en voor het alleen verlenen van beheerderstoegang aan de juiste personen om de integriteit van hun AAD-tenant te behouden. Azure - CUEC: Een gebruikersorganisatie die AAD-services gebruikt, is verantwoordelijk voor het implementeren van geschikte authenticatiemechanismen en het beperken van beheerderstoegang tot de juiste personen om de integriteit van hun SaaS-applicaties te behouden.
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
9.2.5	Beoordeling van toegangsrechten van gebruikers: Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	CA-35.a CA-35.b	OA - 5	Controls aanwezig in assurance rapportage (SOC) In de M365 assurance rapportage is een expliciete control aanwezig omtrent de beoordeling van toegangsrechten die betrekking heeft op privileged/elevated accounts. Daarnaast was voor Teams een bevinding op deze control geconstateerd.	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het inrichten van passende controles over het gebruik van hun Microsoft-accounts en wachtwoorden.
9.2.5.1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld. (BBN 1)	CA-35.a CA-35.b	OA - 5	Controls aanwezig in assurance rapportage (SOC) In de M365 assurance rapportage enkel een expliciete control aanwezig omtrent beoordeling van toegangsrechten die betrekking heeft op privileged/elevated accounts. Daarnaast was voor Teams een bevinding op deze control geconstateerd.	Controls aanwezig in assurance rapportage (SOC)	Zie 9.2.5
9.2.5.2	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.	CA-35.a CA-35.b	OA - 5	Geen controls beschreven Uit assurance rapportages van Azure en M365 is niet op te maken of bevindingen worden behandeld als beveiligingsincidenten. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Eigenaren van M365 assets beoordelen de toegangsrechten van gebruikers ten minste driemaandelijks. Microsoft controleert accounts op naleving van de vereisten voor accountbeheer. Er wordt een ticket geopend voor elke beveiligingsgroep waarmee servicetoegang wordt verleend en de eigenaar van de beveiligingsgroep controleert het lidmaatschap op juistheid. Als afwijkingen worden gevonden, dan worden deze in het ticket genoteerd en wordt een wijziging doorgevoerd in de accountbeheertool. Azure: Een volledig overzicht van de accounts wordt geanalyseerd met de beheerders van elk geïdentificeerde account. Managers moeten de toegang tot een account opnieuw valideren om actief te blijven. Als een beheerder aangeeft dat een account niet meer nodig is, of een beheerder reageert niet, dan wordt het account gedeactiveerd.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				Uit bovenstaande is niet op te maken of de opvolging van bevindingen wordt behandeld als een beveiligingsincident, waardoor deze in de categorie: “geen controls beschreven” valt.		
9.2.5.3	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld. (BBN 2)	CA-35.a CA-35.b	OA - 5	Controls aanwezig in FedRAMP-raamwerk Voor M365 wordt in de assurance rapportage enkel gesproken over beoordeling van privileged/elevated accounts. Uit assurance rapportages van Azure en M365 niet op te maken of accounts zonder hoge rechten ook worden gereviewd en met welke frequentie. Tevens is een bevinding op deze control aanwezig voor Teams. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Eigenaren van M365 bedrijfsmiddelen beoordelen de toegangsrechten van gebruikers ten minste driemaandelijks. Microsoft controleert accounts op naleving van de vereisten voor accountbeheer. Er wordt een ticket geopend voor elke beveiligingsgroep waarmee servicetoegang wordt verleend en de eigenaar van de beveiligingsgroep controleert het lidmaatschap op juistheid. Als er afwijkingen worden gevonden, worden deze in het ticket genoteerd en wordt een wijziging doorgevoerd in de accountbeheertool. Azure: Een volledig overzicht van de accounts wordt geanalyseerd met de beheerders van elk geïdentificeerde account. Managers moeten de toegang tot een account opnieuw valideren om actief te blijven. Als een beheerder aangeeft dat een account niet meer nodig is, of een beheerder reageert niet, wordt het account gedeactiveerd. Uit bovenstaande is voor M365 niet op te maken of alle de toegangsrechten van alle accounts worden beoordeeld of enkel van de beveiligingsgroepen waarmee service toegang mogelijk is ('…that allows service access'). Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is op te maken dat alle uitgegeven toegangsrechten minimaal één keer per kwartaal worden beoordeeld, zowel voor M365 als voor Azure. Dit is opgenomen onder AC-06.07 in de Azure FedRAMP-rapportage en onder AU-10 in de M365 FedRAMP-rapportage.		Zie 9.2.5

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
9.2.6	Toegangsrechten intrekken of aanpassen: De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	CA-35.a CA-43	OA - 3	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	M365 - CUEC-01: De gebruikersorganisatie is verantwoordelijk voor het op de juiste manier autoriseren van gebruikers die toegang krijgen tot de bronnen en het bewaken van de voortdurende geschiktheid van toegang. M365 - CUEC-06: De gebruikersorganisatie is verantwoordelijk voor het beveiligen van de software en hardware die worden gebruikt om toegang te krijgen tot M365. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het uitschakelen/ verwijderen van accounttoegang tot hun Azure-services bij wijziging of beëindiging van de rol van werknemers en contractanten.
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
9.3.1	Geheime authenticatie-informatie gebruiken: Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	CA-34 CA-41	OA - 4 OA -15	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	M365 - CUEC-02: De gebruikersorganisatie is verantwoordelijk voor het inrichten van controles omtrent het gebruik van systeem-ID's en wachtwoorden. M365 - CUEC-03: De gebruikersorganisatie is verantwoordelijk voor het beheer van het wachtwoord-authenticatiemechanisme van hun gebruikers. Azure - CUEC: Klanten zijn verantwoordelijk voor het inrichten van passende controles over het gebruik van hun Microsoft-accounts en wachtwoorden.
9.3.1.1	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.	CA-34 CA-41	OA - 4 OA -15	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk vast te stellen of medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		Zie 9.3.1

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
9.4.1	Beperking toegang tot informatie: Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	CA-36 CA-40 CA-41	OA - 8 OA - 14 PE - 1 PE - 3 PE - 4	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: Klanten zijn verantwoordelijk voor het implementeren van logische toegangscontroles om redelijke zekerheid te bieden dat ongeautoriseerde toegang tot belangrijke systemen wordt beperkt.
9.4.1.1	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	CA-36 CA-40 CA-41	OA - 8 OA - 14 PE - 1 PE - 3 PE - 4	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	zie 9.4.1
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.	CA-36 CA-40 CA-41	OA - 8 OA - 14 PE - 1 PE - 3 PE - 4	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
9.4.2	Beveiligde inlogprocedures: Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	CA-34 CA-36 CA-40 CA-41	OA - 4 OA - 14 OA - 21	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
9.4.2.1	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	CA-34 CA-36 CA-40 CA-41	OA - 4 OA - 14 OA - 21	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
9.4.2.2	Voor het verlenen van toegang tot het netwerk door externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de	CA-34 CA-36 CA-40 CA-41	OA - 4 OA - 14 OA - 21	Controls aanwezig in ISO control mapping / NIST raamwerk het is niet mogelijk vast te stellen of alle aspecten zoals beschreven zijn geïmplementeerd. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
	leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.			M365: Microsoft documenteert voor elke interconnectie de interfacekenmerken, beveiligingsvereisten en de aard van de gecommuniceerde informatie. Microsoft neemt in overeenkomsten met leveranciers eisen op om de informatiebeveiligingsrisico's die verband houden met informatie- en communicatietechnologiediensten en de toeleveringsketen van producten te adresseren. Microsoft vereist dat derden (externe informatiesysteemdiensten) die betrokken zijn bij M365 een Microsoft Master Vendor Agreement (MMVA) en een Interconnection Security Agreement (ISA) ondertekenen. De MMVA vereist dat de derde partij voldoet aan het toepasselijke M365-beveiligingsbeleid en beveiligingsprocedures implementeert om openbaarmaking van vertrouwelijke M365-informatie te voorkomen. M365 bevat bepalingen in de MMVA en eventuele bijbehorende Statement of Work (SOW) waarbij elke leverancier ingaat op de noodzaak om passende beveiligingscontroles te gebruiken. Leveranciers die gevoelige gegevens verwerken, moeten voldoen aan de privacy praktijken en gegevensbeschermingsvereisten van M365-leveranciers. Microsoft implementeert acquisitiecontrole door handhaving van het Microsoft-beveiligingsbeleid. Het Microsoft-beveiligingsbeleid schrijft voor dat waar een derde partij toestemming heeft om (i) toegang te krijgen tot de informatiemiddelen of informatieverwerkingsfaciliteiten van M365's online services, of deze te beheren, of (ii) producten of services toe te voegen aan de informatie van M365's online services verwerkingsfaciliteiten, moeten er in een formeel contract afspraken worden gemaakt om de verantwoordelijkheid en vereisten voor de beveiliging, vertrouwelijkheid, integriteit en beschikbaarheid van de betrokken informatiemiddelen vast te leggen. Passende beveiligingsnormen worden in de overeenkomst behandeld om een niveau van bescherming te bieden. Azure: Azure implementeert het acquisitiebeheer door het afdwingen van het Microsoft-beveiligingsbeleid. Het Beleid schrijft voor dat waar een derde partij toestemming heeft om (i) toegang te krijgen tot, de informatiemiddelen of informatieverwerkingsfaciliteiten van Microsofts online diensten te openen, te verwerken, te hosten of te beheren, of (ii) producten of diensten toe te voegen aan de informatieverwerkingsfaciliteiten van de online diensten van Microsoft, regelingen moet worden vastgelegd in een formeel contract om de verantwoordelijkheid en vereisten voor de beveiliging, vertrouwelijkheid, integriteit en beschikbaarheid van de betrokken informatiemiddelen te definiëren. Passende beveiligingsstandaarden worden behandeld in de overeenkomst, om een niveau van bescherming te bieden tegen geïdentificeerde risico's dat gelijkwaardig is aan het beveiligingsbeleid van Microsoft. Uit bovenstaande is op te maken dat voor toegang door externe leveranciers rekening wordt		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				gehouden met het afdekken van informatiebeveiligingsrisico's, en dat voorwaarden zijn gesteld waar leveranciers aan moeten voldoen om toegang te krijgen.		
9.4.3	Systeem voor wachtwoordbeheer: Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	CA-34 CA-36 CA-40 CA-41	OA - 4 OA - 14 OA - 15	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het inrichten van passende controles over het gebruik van hun Microsoft-accounts en wachtwoorden. Azure - CUEC: De administrators van de gebruikersorganisatie zijn verantwoordelijk voor de keuze en het gebruik van hun wachtwoorden. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het toezicht op, het beheer en de controle van het gebruik van MFA-services door haar personeel. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het waarborgen van de vertrouwelijkheid van gebruikers-ID's en wachtwoorden die worden gebruikt om toegang te krijgen tot MFA-systemen.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
						Azure - CUEC: De gebruikersorganisatie is ervoor verantwoordelijk dat de gegevens die bij de MFA-service worden ingediend, volledig, nauwkeurig en tijdig zijn.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
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. (BBN 1)	CA-34 CA-36 CA-40 CA-41	OA - 4 OA - 14 OA - 15	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om vast te stellen of alle aspecten zoals beschreven zijn geïmplementeerd. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		Zie 9.4.3
9.4.3.2	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.). (BBN 2)	CA-34 CA-36 CA-40 CA-41	OA - 4 OA - 14 OA - 15	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om vast te stellen of alle aspecten zoals beschreven zijn geïmplementeerd. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		Zie 9.4.3
9.4.3.3	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen. (BBN 2)	CA-34 CA-36 CA-40 CA-41	OA - 4 OA - 14 OA - 15	Ontbreken control in SOC geaccepteerd door werkgroep. Uit assurance rapportages niet op te maken of de eisen aan wachtwoorden geautomatiseerd worden afgedwongen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: M365-wachtwoordbeheersystemen zijn interactief en garanderen kwaliteitswachtwoorden. Voor wachtwoord gebaseerde authenticatie dwingt Microsoft een minimale wachtwoordcomplexiteit af van hoofdlettergevoeligheid, aantal tekens, combinatie van hoofdletters, cijfers en speciale tekens, inclusief minimumvereisten voor elk type. Microsoft gebruikt Active Directory om de handhaving van ons wachtwoordbeleid te beheren. M365-systemen zijn geconfigureerd om gebruikers te dwingen complexe wachtwoorden te gebruiken. Aan wachtwoorden wordt een maximumleeftijd en een minimumlengte van tekens toegekend. Vereisten voor wachtwoordverwerking omvatten het wijzigen van door de contractant verstrekte standaardwachtwoorden voordat de bijbehorende service of het bijbehorende systeem wordt geïntroduceerd in een M365-omgeving die eigendom is of wordt beheerd. Elk M365-team heeft een lokale beheerderswachtwoordbeheerder om lokale beheerderswachtwoorden voor servicesystemen veilig te onderhouden en op te slaan. Azure: Waar wachtwoorden worden gebruikt, gebruikt Azure Active Directory om te bepalen of wachtwoord authenticators voldoende sterk zijn om te voldoen aan de wachtwoordlengte,		Zie 9.4.3

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				complexiteit, rotatie en levensduurbeperkingen. Active Directory zorgt ervoor dat de sterkte van de wachtwoord authenticator bij het maken voldoende is. Uit bovenstaande is op te maken dat de eisen aan wachtwoorden geautomatiseerd worden afgedwongen. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien het aantonen van deze maatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
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.	CA-34 CA-36 CA-40 CA-41	OA - 4 OA - 14 OA - 15	Controls aanwezig in ISO control mapping / NIST raamwerk Het is niet mogelijk om op te maken wat de geldigheidsduur is van initiële wachtwoorden en wachtwoorden die gereset zijn. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft controleert de toewijzing van geheime authenticatie-informatie via een formeel beheerproces. Microsoft beheert authenticators van M365-informatiesystemen door administratieve procedures vast te stellen en te implementeren voor de initiële distributie van authenticators, voor verloren, gecompromitteerde of beschadigde authenticators en voor het intrekken van authenticators. De leidinggevende van de medewerker ontvangt een eenmalig wachtwoord, dat vertrouwelijk aan de medewerker wordt gecommuniceerd. Bij de eerste aanmelding moet de werknemer het wachtwoord wijzigen in overeenstemming met de ontwerpcriteria voor wachtwoorden. Regelmatige door het systeem afgedwongen wachtwoordupdates worden gemaakt op basis van beleid. Azure: Op het moment dat het account voor het eerst wordt gemaakt, wijst Active Directory een unieke identificatie en willekeurig tijdelijk wachtwoord toe die voldoet aan de beleidsvereisten van Microsoft Corporate en Azure. Active Directory behoudt de unieke identificatie die aan het account is gekoppeld gedurende de levensduur van het account. Accountidentificatie wordt nooit herhaald binnen Active Directory. Na goedkeuring van het aanmaken van een account van zijn/haar manager, ontvangt een nieuwe gebruiker een e-mail van MyAccess met betrekking tot haar of zijn verzoek. Deze e-mail heeft een URL-verwijzing naar een uniek gegenereerde pagina om een tijdelijk wachtwoord te krijgen. Dit wachtwoord wordt willekeurig gegenereerd en kan na één (1) dag opnieuw worden ingesteld. Het initiële gegenereerde wachtwoord is in overeenstemming met de basisvereisten van Azure Identity Management, inclusief vereisten voor complexiteit en lengte. Nadat de smartcard aan de gebruiker is verstrekt, stuurt het C+AI Security Smart Card-ondersteuningspersoneel een e-mail met een eerste pincode voor de smartcard die moet worden gereset. Bepaalde domeinen hebben geen wachtwoord - de pincode van de smartcard is de authenticatiemethode voor het account.		Zie 9.4.3

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				De initiële procedures voor het distribueren van authenticatoren zijn hierboven vermeld. Als een authenticator zoekraakt of wordt gecompromitteerd, stellen Azure-beheerders de authenticator opnieuw in, geven deze opnieuw uit of trekken deze in. Uit bovenstaande is op te maken dat initiële wachtwoorden van M365 bij het eerste gebruik gewijzigd moeten worden. Echter is voor M365 niet op te maken wat de maximale geldigheidsduur van het initiële wachtwoord is. Voor Azure is uit bovenstaande niet duidelijk op te maken wat de maximale geldigheidsduur van het initiële wachtwoord is en of wordt afgedwongen dat deze bij het eerste gebruik wordt gewijzigd.		
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.	CA-34 CA-36 CA-40 CA-41	OA - 4 OA - 14 OA - 15	Ontbreken control in SOC geaccepteerd door werkgroep. Het is in assurance rapportages niet opgenomen of de geldigheidsduur van wachtwoorden voldoet, wel is vastgesteld dat de bovenliggende BIO-control voldoet. Daarnaast is in de assurance rapportages opgenomen dat Microsoft voor beheer gebruikmaakt van Just In Time-toegang. Daarmee is deze overheidsmaatregel minder relevant. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		Zie 9.4.3
9.4.4	Speciale systeemhulpmiddelen gebruiken: Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	CA-48 CA-60	VM - 1 VM - 2 VM - 9	Controls aanwezig in ISO control mapping / NIST raamwerk Toegang tot systeemhulpmiddelen wordt niet expliciet opgenomen in de assurance rapportages en/of controls. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Hieruit is op te maken dat voor M365 specifiek aandacht is besteed aan systeemhulpmiddelen. Hieruit is echter niet duidelijk op te maken dat dit alleen door bevoegd personeel gebruikt mag wordt. Voor Azure is op te maken dat alle verhoogde toegangsrechten worden aangevraagd, echter is hieruit niet duidelijk op te maken hoe dit ingericht is voor systeemhulpmiddelen en welk personeel daar toegang toe heeft (zie ook 9.4.4.1). Tevens is hieruit niet duidelijk op te maken of het gebruik van deze systeemhulpmiddelen gelogd wordt, en hoe lang deze logging beschikbaar is voor onderzoek (zie ook 9.4.4.2).		
9.4.4.1	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.	CA-48 CA-60	VM - 1 VM - 2 VM - 9	Controls aanwezig in ISO control mapping / NIST raamwerk Toegang tot systeemhulpmiddelen wordt niet expliciet opgenomen in assurance rapportages. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				M365: Microsoft beperkt en controleert streng het gebruik van hulpprogramma's die mogelijk systeem- en toepassingscontroles kunnen overschrijven. Microsoft vereist dat gebruikers van informatiesysteemaccounts of -rollen, met toegang tot beveiligingsfuncties of beveiligingsrelevante informatie, niet-bevoorrechte accounts of rollen gebruiken bij toegang tot niet-beveiligingsfuncties. Niet-geprivilegieerde acties (bijvoorbeeld gebruik van webbrowsers, e-mailclients, etc.) zijn niet toegestaan binnen de productieomgeving. Azure: Azure-personeel heeft standaard geen permanente verhoogde toegang tot de Azure-productieomgeving. Azure vereist dat gebruikers hun accounts gebruiken voor specifieke taakfuncties waarvoor het juiste toegangsniveau is vereist. Verhoogde toegang wordt alleen gebruikt voor de gespecificeerde functiefuncties die vereist zijn door de verantwoordelijkheden van de gebruiker; tijdelijke verhoogde toegang wordt verleend via JIT op basis van een geldige zakelijke rechtvaardiging. Permanente verhoogde toegang in de vorm van noodtoegangsaccounts is niet toegestaan, behalve voor het beheer en de werking van het systeem. Daarnaast zijn binnen de productieomgeving geen onbevoegde handelingen zoals het gebruik van webbrowsers, e-mailclients, etc. toegestaan. Uit bovenstaande is op te maken dat voor M365 specifieke aandacht is besteed aan systeemhulpmiddelen. Hieruit is echter niet duidelijk op te maken dat dit alleen door bevoegd personeel gebruikt mag wordt. Voor Azure is op te maken dat alle verhoogde toegangsrechten worden aangevraagd, echter is hieruit niet duidelijk op te maken hoe dit ingericht is voor systeemhulpmiddelen en welk personeel daar toegang toe heeft.		
9.4.4.2	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	CA-48 CA-60	VM - 1 VM - 2 VM - 9	Geen controls beschreven Het gebruik van systeemhulpmiddelen wordt niet expliciet opgenomen in de assurance rapportages en/of controls. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Hieruit is niet duidelijk op te maken of het gebruik van deze systeemhulpmiddelen gelogd wordt, en hoe lang deze logging beschikbaar is voor onderzoek.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
9.4.5	Toegangsbeveiliging op programmabroncode: Toegang tot de programmabroncode behoort te worden beperkt.	CA-19 CA-35.a CA-36 CA-38	SDL - 5	Controls aanwezig in FedRAMP-raamwerk Beperking van toegang tot broncode is niet expliciet opgenomen, wel impliciet door beveiligingsmaatregelen voor productie en development. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is op te maken dat gebruik wordt gemaakt van het 'least privilege' concept is het toewijzen van rollen en rechten aan gebruikers binnen Microsoft. Dit is opgenomen onder AC-6 in de M365 FedRAMP-rapportage. Door het hanteren van “least privilege” is op te maken dat toegang tot de programmabroncode wordt beperkt.	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
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.	CA-44 CA-54 CA-62 CA-64	DS - 1 DS - 4 *EKM-01* *EKM-04*	Controls aanwezig in ISO control mapping / NIST raamwerk Beleid omtrent cryptografische maatregelen is niet expliciet opgenomen in assurance rapportage, wel impliciet door aanwezige maatregelen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Microsoft heeft een beleid ontwikkeld en geïmplementeerd voor het gebruik van cryptografische controles voor de bescherming van M365-informatie. Versleutelingsmechanismen en -technieken die door de M365-teams worden gebruikt, volgen de vereisten en beperkingen die zijn uiteengezet in het M365-informatiebeveiligingsbeleid. Uit bovenstaande is op te maken dat beleid aanwezig is omtrent het gebruik van cryptografische toepassingen.	Controls aanwezig in assurance rapportage (SOC)	M365 - CUEC-04: De gebruikersorganisatie is verantwoordelijk voor het afdwingen van het gewenste versleutelingsniveau voor netwerk-sessies. M365 - CUEC-06: De gebruikersorganisatie is verantwoordelijk voor het beveiligen van de software en hardware die worden gebruikt om toegang te krijgen tot M365. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het bepalen, implementeren en beheren van versleutelingsvereisten voor haar gegevens binnen het Azure-platform waar Azure dit niet standaard inschakelt en/of dit door de gebruikersorganisatie kan worden beheerd.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
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.	CA-44 CA-54 CA-62 CA-64	DS - 1 DS - 4 *EKM-01* *EKM-04*	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk expliciet vast te stellen of alle aspecten van cryptografiebeleid zoals beschreven zijn geïmplementeerd. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		Zie 10.1.1
10.1.1.2	Cryptografische toepassingen voldoen aan passende standaarden.	CA-44 CA-54 CA-62 CA-64	DS - 1 DS - 4 *EKM-01* *EKM-04*	Controls aanwezig in ISO control mapping / NIST raamwerk Uit assurance rapportages van Azure en M365 is niet op te maken aan welke standaard de cryptografische toepassingen voldoen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Microsoft heeft een beleid ontwikkeld en geïmplementeerd voor het gebruik van cryptografische controles voor de bescherming van M365-informatie. Versleutelingsmechanismen en -technieken die door de M365-teams worden gebruikt, volgen de vereisten en beperkingen die zijn uiteengezet in het M365-informatiebeveiligingsbeleid. Servicegegevens en -informatie worden behandeld in overeenstemming met de vereisten en beperkingen die zijn gespecificeerd in de Asset Classification and Data Handling Standards wanneer cryptografie wordt gebruikt. Cryptografische controles zijn ontworpen en geïmplementeerd om de vertrouwelijkheid, integriteit en beschikbaarheid van M365-informatie te beschermen. Microsoft biedt digitale certificaten op openbare websites. M365-ondersteuningspersoneel gebruikt TLS-codering (FIPS 140-2 Level 2 gevalideerd) voor verbindingen die buiten de grenzen van M365 vallen. TLS maakt gebruik van cryptografische mechanismen waarmee client-/servertoepassingen via het netwerk kunnen communiceren op een manier die is ontworpen om afluisteren en knoeien. Zie FIPS 140-validatie (https://technet.microsoft.com/en-us/library/security/cc750357.aspx) voor meer informatie. Azure: Voor alle asset types gebruikt Azure cryptografische controles om de vertrouwelijkheid, authenticiteit en integriteit van gevoelige gegevens te beschermen tijdens verzending of in rust. Om de vertrouwelijkheid te waarborgen, gebruikt Azure zowel		Zie 10.1.1

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				symmetrische als asymmetrische sleutels voor het versleutelen van gevoelige gegevens om toegang door onbevoegde partijen te voorkomen. TLS 1.2-codering voor toegang. Versleuteling is vereist voor alle verbindingen. PKI-certificaten worden gebruikt binnen Azure op de interne RD-gateways en worden verkregen via de Azure PKI, en SSL-certificaten die worden gebruikt door toegangsoplossingen. Versleutelingsmechanismen en -technieken die door de Azure-serviceteams worden gebruikt, volgen de vereisten en beperkingen die zijn beschreven in de Microsoft Key Management Standard, Microsoft Operational Encryption Standard, Azure Cryptographic Controls Standard Operating Procedure. Uit bovenstaande is op te maken dat beleid aanwezig is omtrent het gebruik van cryptografische toepassingen. Tevens is hieruit op te maken dat verschillende versleutelingsmechanismen en -technieken gebruikt worden. Hieruit is echter niet exact op te maken welke standaarden (op dit moment) worden gehanteerd. Per interview met Microsoft hebben wij vernomen dat in de online beschikbare documentatie tevens informatie is opgenomen omtrent de toegepaste cryptografische maatregelen, zowel voor Teams als voor Azure AD.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
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.	n.v.t.	DS - 1 DS - 4	Controls aanwezig in FedRAMP-raamwerk In de assurance rapportage zijn geen specifieke controls opgenomen over sleutelbeheer. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is op te maken dat M365 encryptie gebruikt om ongeoorloofde openbaarmaking van informatie te voorkomen en wijzigingen in informatie tijdens verzending te detecteren. M365 biedt specifiek FIPS 140-2-compatibele versleutelingen, waaronder integriteitsvalidatie voor klantverbindingen, onderling verbonden systeemverbindingen en RAS-verbindingen met M365. Voor verbindingen met klanten is M365 geconfigureerd om te onderhandelen over FIPS-compatibele TLS 1.2-protocollen met ondersteunde clientbrowsers, hoewel niet-FIPS-compatibele protocollen worden ondersteund voor ondersteuning van oudere browsers. Verbindingen met onderling verbonden systemen worden gemaakt met behulp van strikt afgedwongen FIPS-compatibele TLS 1.2-protocollen. Verbindingen voor externe toegang van M365-serviceteambeheerders worden gemaakt met behulp van strikt afgedwongen FIPS-compatibele TLS 1.2-protocollen. Dit is opgenomen onder AC-6 in de M365 FedRAMP-rapportage.	Controls aanwezig in assurance rapportage (SOC)	M365 - CUEC-04: De gebruikersorganisatie is verantwoordelijk voor het afdwingen van het gewenste versleutelingsniveau voor netwerk-sessies. M365 - CUEC-06: De gebruikersorganisatie is verantwoordelijk voor het beveiligen van de software en hardware die worden gebruikt om toegang te krijgen tot M365. M365 - CUEC-10/Azure: De gebruikersorganisatie is verantwoordelijk voor het begrijpen en naleven van de inhoud van hun servicecontracten, inclusief verplichtingen met betrekking tot systeembeveiliging, beschikbaarheid, verwerkingsintegriteit en vertrouwelijkheid. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het bepalen, implementeren en beheren van versleutelingsvereisten voor haar gegevens

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
						binnen het Azure-platform waar Azure dit niet standaard inschakelt en/of dit door de gebruikersorganisatie kan worden beheerd.
10.1.2.1		n.v.t.				Zie 10.1.2

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
	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.		DS - 1 DS - 4	Controls aanwezig in ISO control mapping / NIST raamwerk Uit assurance rapportages van Azure en M365 niet op te maken welke standaarden gehanteerd worden voor het beheer van cryptografische sleutels. Daarnaast voor M365 geen specifieke assurance rapportage control voor het beheer van sleutels. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft heeft een beleid ontwikkeld en geïmplementeerd met betrekking tot het gebruik, de bescherming en de levenscyclus van cryptografische sleutels. Microsoft stelt en beheert cryptografische sleutels voor de vereiste cryptografie die binnen het informatiesysteem wordt gebruikt in overeenstemming met gedefinieerde vereisten voor het genereren, distribueren, opslaan, openen en vernietigen van sleutels. In overeenstemming met het beveiligingsbeleid van Microsoft en M365 gebruikt M365 de cryptografische mogelijkheden die zijn ingebouwd in het Windows-besturingssysteem voor certificaten en authenticatiemechanismen (bijv. Kerberos). Deze cryptografische modules zijn door NIST gecertificeerd als FIPS 140-2 gevalideerd. Relevante NIST-certificaatnummers voor Microsoft zijn te vinden op FIPS 140-1 en FIPS 140-2 List (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm). Telkens wanneer cryptografische mogelijkheden worden gebruikt om de vertrouwelijkheid, integriteit of beschikbaarheid van gegevens binnen M365 te beschermen, zijn de gebruikte modules en codes FIPS 140-2 gevalideerd. Zie FIPS 140-validatie (http://technet.microsoft.com/en-us/library/cc750357.aspx) voor meer informatie. Azure produceert, beheert en distribueert symmetrische cryptografische sleutels met behulp van NIST FIPS-compatibele technologie en proces voor sleutelbeheer. C+AI Security heeft aanvullende normen gepubliceerd die de implementatie van systemen en besturingselementen voor communicatiebeveiliging in de Azure-omgeving vergemakkelijken en ondersteunen. Deze documenten omvatten: - Azure Access Control SOP - Azure Asset Management-SOP - Azure cryptografisch beheer SOP - Key Management Standard - Asset Classification Standard - Asset Protection Standards Uit bovenstaande is niet op te maken of de PKI-Overheid-eisen en/of de ISO-11770 standaard voor het beheer van cryptografische sleutels wordt gehanteerd.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
10.1.2.2	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.	n.v.t	DS - 1 DS - 4	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om vast te stellen of er afspraken zijn over reservecertificaten van een alternatieve leverancier. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		Zie 10.1.2
11.1.1	Fysieke beveiligingszone: Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	CA-17	PE - 1	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Algemeen - CUEC: De gebruikersorganisatie is verantwoordelijk voor het definiëren van de eigen beveiligingszones om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten: gebruikers dienen zich bewust te zijn van de locatie van hun werkplek en de daaraan verbonden risico's (bijvoorbeeld bij werken op afstand van kantoor).
11.1.1.1	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.	CA-17	PE - 1	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Zie 11.1.1
11.1.2	Fysieke toegangsbeveiliging: Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	zie Azure	PE - 1 PE - 2 PE - 3 PE - 4	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
11.1.2.1	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	Zie Azure	PE - 1 PE - 2 PE - 3 PE - 4	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om vast te stellen dat in geval van concrete beveiligingsrisico's waarschuwingen, conform onderlinge afspraken, worden verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		Zie 11.1.2
11.1.3	Kantoren, ruimten en faciliteiten beveiligen: Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	CA-17	PE - 1 PE - 4	Controls aanwezig in ISO control mapping / NIST raamwerk Fysieke beveiliging van o.a. Microsoft kantoren wordt niet genoemd in de controls. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365. Hieruit is op te maken dat Microsoft fysieke beveiliging ontwerpt en toepast voor kantoren, kamers en faciliteiten. Microsoft biedt beveiligingsmaatregelen om de toegang tot gebieden binnen de faciliteit die officieel als openbaar toegankelijk zijn aangemerkt, te controleren. Microsoft-datacenters gebruiken fysieke toegangsapparaten zoals perimeterpoorten, elektronische toegangsbadgelezers, biometrische lezers, mantraps, anti-achterklepapparaten en anti-passback-controles, evenals beveiligingsfunctionarissen om de toegang tot de datacenters te controleren. Uit bovenstaande is op te maken dat fysieke beveiliging wordt ontwerpen en toegepast.	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
11.1.3.1	Sleutelbeheer is ingericht op basis van een sleutelplan.	CA-17	PE - 1 PE - 4	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om vast te stellen of sleutelbeheer is ingericht op basis van een sleutelplan. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
11.1.4	Beschermen tegen bedreigingen van buitenaf: Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	CA-26 CA-27 CA-29 CA-30 CA-38 CA-47 CA-48 CA-50 CA-53	BC - 9 DS - 5 DS - 6 DS - 14 PE - 7 PE - 8	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	M365 - CUEC-07: De gebruikersorganisatie is verantwoordelijk voor het geven van trainingen aan eindgebruikers. M365 - CUEC-08: De gebruikersorganisatie is verantwoordelijk voor het melden van geïdentificeerde beveiligings-, beschikbaarheids-, verwerkingsintegriteits- en vertrouwelijkheidsproblemen.
11.1.4.1	De organisatie heeft geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.	CA-26 CA-27 CA-29 CA-30 CA-38 CA-47 CA-48 CA-50 CA-53	BC - 9 DS - 5 DS - 6 DS - 14 PE - 7 PE - 8	Controls aanwezig in FedRAMP-raamwerk Het is niet mogelijk om op te maken of deze maatregelen zijn genomen op basis van een expliciete risicoafweging. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Uit bovenstaande is voor M365 en Azure niet op te maken of deze maatregelen zijn genomen op basis van een expliciete risico afweging. Uit aanvullende ontvangen FedRAMP-rapportages (geen assurance) is op te maken dat (beveiligingsmaatregelen voor) bedreigingen van buitenaf zijn opgenomen in de Microsoft		Zie 11.1.4

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				Security Policy (MSP) en de Microsoft Security Program Policy (MSPP). Deze documenten worden beoordeeld door het Microsoft Information Risk Management Council, waaruit op te maken is dat hierbij een expliciete risicoafweging van toepassing is. Dit is opgenomen onder PE-01 in de Azure FedRAMP-rapportage en PE-1 in de M365 FedRAMP-rapportage.		
11.1.4.2	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.	CA-26 CA-27 CA-29 CA-30 CA-38 CA-47 CA-48 CA-50 CA-53	BC - 9 DS - 5 DS - 6 DS - 14 PE - 7 PE - 8	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Zie 11.1.4
11.1.5	Werken in beveiligde gebieden: Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	CA-17	PE - 1 PE - 3 PE - 4	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
11.1.6	Laad- en loslocatie: Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	Zie Azure	PE - 5	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
11.2.1	Plaatsing en bescherming van apparatuur: Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	Zie Azure	PE - 4 PE - 7	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
11.2.2	Nutsvoorzieningen: Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Zie Azure	PE - 7	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
11.2.3	Beveiliging van bekabeling: Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.	Zie Azure	PE - 6 PE - 7	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
11.2.4	Onderhoud van apparatuur: Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Zie Azure	PE - 6 PE - 7	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
11.2.5	Verwijdering van bedrijfsmiddelen: Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	Zie Azure	SOC2 - 3 DS - 10 DS - 12	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein: Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	CA-17	SOC2 - 3 DS - 10 DS - 12 *DCS-04* *DCS-05*	Controls aanwezig in ISO control mapping / NIST raamwerk In de assurance rapportage is geen expliciete control opgenomen voor het beveiligen van apparatuur buiten het terrein. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft de ISO27001-certificering (2016) voor M365. Hieruit is op te maken dat Microsoft beveiliging toepast op off-site bedrijfsmiddelen, rekening houdend met de verschillende risico's van werken buiten de gebouwen van de organisatie. Microsoft implementeert cryptografische mechanismen om de vertrouwelijkheid en integriteit te beschermen van informatie die is opgeslagen op digitale media tijdens transport buiten gecontroleerde gebieden. Het gebruik of de opslag van door Microsoft beheerde informatieverwerkingsapparatuur en/of media met High Business Impact (HBI) of Medium Business Impact (MBI)-gegevens (zoals gedefinieerd in het Microsoft-beveiligingsbeleid) buiten een door Microsoft Online Services beheerde faciliteit moet worden goedgekeurd door de eigenaar(s) van bedrijfsmiddelen. De bescherming die wordt geboden aan apparatuur en/of media die zich buiten een door Microsoft Online Services beheerde faciliteit bevinden, is evenredig met de bescherming die wordt geboden aan apparatuur en media die zich in een door Microsoft beheerde faciliteit bevindt. Hieruit is op te maken dat bedrijfsmiddelen buiten het terrein worden beveiligd, waarbij rekening wordt gehouden met verschillende risico's van werken buiten het terrein van de organisatie.	Controls aanwezig in FedRAMP-raamwerk In de assurance rapportage is geen expliciete control opgenomen voor de beveiliging van apparatuur buiten het terrein. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is op te maken dat beveiligingsmaatregelen worden getroffen voor backup tapes die zich buiten het terrein bevinden. Dit is opgenomen onder CP-09 in de Azure FedRAMP-rapportage. Tevens is op te maken dat Azure-personeel niet reist met apparaten die zich in de Azure-inventaris bevinden. Hieruit is niet op te maken of controls geformuleerd zijn omtrent beveiliging van overige apparatuur en bedrijfsmiddelen buiten het terrein. Tevens is hieruit niet op te maken of hierbij rekening wordt gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
11.2.7	Veilig verwijderen of hergebruiken van apparatuur: Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	n.v.t.	SOC2 - 3 DS - 10 DS - 12	Controls aanwezig in ISO control mapping / NIST raamwerk Uit controls niet op te maken of alle onderdelen van de apparatuur die opslagmedia bevatten worden geverifieerd voorafgaand aan verwijdering of hergebruik. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft verifieert apparatuur die opslagmedia bevat om ervoor te zorgen dat gevoelige gegevens en software zijn verwijderd of veilig zijn overschreven voordat ze worden weggegooid of hergebruikt. Microsoft maakt gebruik van opschoningsmechanismen met een sterkte en integriteit die in overeenstemming zijn met de beveiligingscategorie of classificatie van de informatie. Microsoft gebruikt eenheden en processen voor het wissen van gegevens om gegevens op te schonen en op te schonen op een manier die consistent is met NIST SP 800-88, en die in overeenstemming is met de Microsoft-activaclassificatie van het bedrijfsmiddel. Voor bedrijfsmiddelen die moeten worden vernietigd, maakt Microsoft gebruik van services voor de vernietiging van bedrijfsmiddelen op locatie. Azure: Azure digitale media-assets worden beschermd in Azure-datacenters en GC3's via fysieke toegangscontroles en logische toegangscontroles voor de levensduur van de asset. Azure-assets worden gewist, opgeschoond of vernietigd met de methoden NIST SP 800-88 Revisie 1 voordat de asset opnieuw wordt gebruikt of verwijderd. Azure maakt gebruik van dataverwijderingseenheden van Blancco. Blancco ondersteunt de NIST SP 800-88-vereisten voor opschonen en opschonen/veilig wissen. Voor de vernietiging van activa maakt Azure gebruik van services voor de vernietiging van activa op locatie. Hieruit is op te maken dat processen aanwezig zijn voor het opschonen/veilig wissen van apparatuur voor verwijderen of hergebruik.		
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
11.2.8	Onbeheerde gebruikersapparatuur: Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	CA-17	LA - 5 CCM - 2 PE - 4	Controls aanwezig in ISO control mapping / NIST raamwerk Onbeheerde gebruikersapparatuur niet expliciet benoemd in assurance rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. Microsoft voorkomt toegang tot het systeem door een sessievergrendeling te starten na een periode van inactiviteit of na ontvangst van een verzoek van een gebruiker. Microsoft heeft beleid geïmplementeerd dat vereisten voor sessietime-out in Office afdwingt. Hieruit is op te maken dat onbeheerde gebruikersapparatuur beschermd is.	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het implementeren van time-out voor werkstations voor langere perioden van inactiviteit.
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
11.2.9	‘Clear desk’- en ‘clear screen’-beleid: Er behoort een ‘clear desk’-beleid voor papieren documenten en verwijderbare opslagmedia en een ‘clear screen’-beleid voor informatieverwerkende faciliteiten te worden ingesteld.	CA-36 CA-40	LA - 5 CCM - 2 PE - 4	Controls aanwezig in ISO control mapping / NIST raamwerk Cleardesk- en clearscreen policy niet expliciet benoemd in assurance rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. Hieruit is op te maken dat o.a. een automatische vergrendeling van 15 minuten voor sessie-inactiviteit is geïmplementeerd voor systemen, waarbij het lockscreen wordt getoond.	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het implementeren van time-out voor werkstations voor langere perioden van inactiviteit.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
11.2.9.1	Een onbemensde werkplek is altijd vergrendeld.	CA-36 CA-40	LA - 5 CCM - 2 PE - 4	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om vast te stellen dat een onbemensde werkplek altijd vergrendeld is, wel is een inactivity periode van kracht. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
11.2.9.2	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.	CA-36 CA-40	LA - 5 CCM - 2 PE - 4	Controls aanwezig in ISO control mapping / NIST raamwerk Uit assurance rapportages van Azure en M365 niet op te maken of een screensaver met inactiviteit van maximaal 15 minuten aanwezig is. Daarnaast in M365 assurance rapportage geen control voor een policy voor cleardesk en clearscreen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: er is een automatische vergrendeling van 15 minuten voor sessie-inactiviteit geïmplementeerd voor systemen, waarbij het lockscreen wordt getoond. Azure: Azure beëindigt automatisch Microsoft-gebruikerssessies na ontvangst van een uitlogverzoek van de gebruiker. Secure Admin Workstations (SAW's) moeten opnieuw worden geverifieerd na maximaal tien (10) minuten inactiviteit van de gebruiker. De SAW VPN beëindigt inactieve sessies na driehonderdzestig (360) minuten inactiviteit, en de niet-SAW VPN beëindigt inactieve sessies na zestig (60) minuten inactiviteit. Servers: RDP en SSH time-out bij inactiviteit nemen de instellingen van de doelserver over. Azure-servers zijn geconfigureerd om inactieve sessies te beëindigen na vijftien (15) minuten inactiviteit. Netwerkapparaten: SSH-time-out voor inactiviteit neemt de instellingen van het doelnetwerkapparaat over. Azure-netwerkapparaten zijn geconfigureerd om inactieve sessies na zestig (60) minuten te beëindigen. Uit bovenstaande is op te maken dat voor M365 en Azure inactiviteit timers zijn geïmplementeerd voor het systeem, systeemcomponenten en netwerkcomponenten.		Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het implementeren van time-out voor werkstations voor langere perioden van inactiviteit.
11.2.9.3	Sessies op remote desktops worden op het remote platform vergrendeld na een vastgestelde periode.	CA-36 CA-40	LA - 5 CCM - 2 PE - 4	Controls aanwezig in ISO control mapping / NIST raamwerk Uit assurance rapportages van Azure en M365 niet op te maken of een screensaver met inactiviteit van maximaal 15 minuten aanwezig is. Daarnaast in M365 assurance rapportage geen control voor een policy voor cleardesk en clearscreen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: er is een automatische vergrendeling van 15 minuten voor sessie-inactiviteit geïmplementeerd voor systemen, waarbij het lockscreen wordt getoond.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				Azure: Azure beëindigt automatisch Microsoft-gebruikerssessies na ontvangst van een uitlogverzoek van de gebruiker. Secure Admin Workstations (SAW's) moeten opnieuw worden geverifieerd na maximaal tien (10) minuten inactiviteit van de gebruiker. De SAW VPN beëindigt inactieve sessies na driehonderdzestig (360) minuten inactiviteit, en de niet-SAW VPN beëindigt inactieve sessies na zestig (60) minuten inactiviteit. Servers: RDP en SSH time-out bij inactiviteit nemen de instellingen van de doelserver over. Azure-servers zijn geconfigureerd om inactieve sessies te beëindigen na vijftien (15) minuten inactiviteit. Netwerkapparaten: SSH-time-out voor inactiviteit neemt de instellingen van het doelnetwerkapparaat over. Azure-netwerkapparaten zijn geconfigureerd om inactieve sessies na zestig (60) minuten te beëindigen. Uit bovenstaande is op te maken dat voor M365 en Azure inactiviteit timers zijn geïmplementeerd voor het systeem, systeemcomponenten en netwerkcomponenten.		
11.2.9.4	Het overnemen van sessies op remote werkplekken op een andere werkplek is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd. Na een expliciete risicoafweging mag hiervan worden afgeweken.	CA-36 CA-40	LA - 5 CCM - 2 PE - 4	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om expliciet vast te stellen welke inlogprocedure van toepassing is bij het overnemen van sessies op remote werkplekken. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
11.2.9.5	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van de token de toegangsbeveiligingslock automatisch geactiveerd.	CA-36 CA-40	LA - 5 CCM - 2 PE - 4	Geen controls beschreven Uit assurance rapportages van Azure en M365 niet op te maken of gebruik wordt gemaakt van chipcardtokens. Daarnaast in M365 assurance rapportage geen control voor een policy voor cleardesk en clearscreen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Hieruit is niet op te maken of de beveiligingslock wordt geactiveerd bij het verwijderen van de token (smartcard).		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.1.1	Gedocumenteerde bedieningsprocedures: Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	CA-01 CA-0 CA-26 CA-47 CA-49	DS - 10 DS - 12 SOC2 - 7 C5 - 1 VM - 5 VM - 6 VM - 13 IM - 3 CM -1	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.1.2	Wijzigingsbeheer: Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	CA-03 CA-11 CA-14 CA-18 CA-19 CA-20 CA-21 CA-46	CM - 1 CM - 2 CM - 3 CM - 4 CM - 5 CM - 6 CM - 7 CM - 8	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het volgen van een Secure Development Lifecycle-methodologie voor haar applicaties die zijn ontwikkeld op Azure. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor de kwaliteitsborging van de applicatie voordat deze naar de Azure-productieomgeving wordt gebracht. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het bewaken van de beveiliging van haar applicaties die op Azure zijn ontwikkeld.
12.1.2.1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: (a) het administreren van wijzigingen; (b) risicoafweging van mogelijke gevolgen van de wijzigingen; (c) goedkeuringsprocedure voor wijzigingen.	CA-03 CA-11 CA-14 CA-18 CA-19 CA-20 CA-21 CA-46	CM - 1 CM - 2 CM - 3 CM - 4 CM - 5 CM - 6 CM - 7 CM - 8	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om op te maken of de procedure voor wijzigingsbeheer alle aspecten zoals genoemd in de beheersmaatregel benoemt. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft beheert wijzigingen in zijn organisatie, bedrijfsprocessen, informatieverwerkingsfaciliteiten en systemen die van invloed zijn op informatiebeveiliging. Microsoft implementeert goedgekeurde gecontroleerde wijzigingen in het M365-		Zie 12.1.2

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				informatiesysteem. Er is een operationele procedure voor wijzigingsbeheer voor M365 en gerelateerde systeemwijzigingen. Deze procedure omvat een proces voor de beoordeling en goedkeuring door het management van M365. Deze procedure voor wijzigingsbeheer wordt gecommuniceerd aan partijen die systeemonderhoud uitvoeren op of in een M365-faciliteit. De operationele wijzigingscontroleprocedure houdt rekening met de volgende acties: - De identificatie en documentatie van de geplande wijziging - Een beoordelingsproces van mogelijke veranderingsimpact - Wijzigingstesten in een goedgekeurde niet-productieomgeving - Wijzig communicatieplan - Goedkeuringsproces voor wijzigingsbeheer - Afbreken en herstelplan wijzigen (indien van toepassing) M365 richt zich op informatiebeveiliging in projectmanagement, ongeacht het type project. De implementatie van levenscyclusondersteuning door M365 wordt beschreven in Microsoft's Security Development Lifecycle (SDL), een proces dat wordt gevolgd door M365-engineering- en ontwikkelingsprojecten. Voor ontwikkelingsprojecten moet een analyse van beveiligingsvereisten worden voltooid. Dit analysedocument fungeert als een raamwerk en omvat de identificatie van mogelijke risico's voor het voltooide ontwikkelingsproject, evenals mitigatiestrategieën die tijdens de ontwikkelingsfasen kunnen worden geïmplementeerd en getest. Tijdens de ontwikkelingslevenscyclus worden kritische veiligheidscontroles en goedkeuringscontroles opgenomen. Azure: Azure-serviceteams gebruiken Azure DevOps of IcM voor het bijhouden van wijzigingsbeheer, waarbij broncode en werkitems met betrekking tot configuratiebasislijnen en configuratie-instellingen worden bijgehouden. Werkitems en broncodewijzigingen documenteren bewijs van goedkeuringen en volgen alle wijzigingen die zijn aangebracht om een nieuwe configuratie-instelling vrij te geven. Alle wijzigingen onder configuratiebeheer aan Azure-assets worden beoordeeld en goedgekeurd of afgekeurd met expliciete aandacht voor de analyse van de beveiligingsimpact. Volgens de Microsoft Change Management Standard vereisen alle wijzigingen gedocumenteerde testprocedures. Uit bovenstaande is op te maken dat minimaal aandacht wordt besteed aan het administreren van wijzigingen, risico-afwegingen en goedkeuring van wijzigingen. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien het aantonen van deze maatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.1.3	Capaciteitsbeheer: Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	CA-29 CA-30 CA-31 CA-61	BC - 10 CCM - 5	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen: Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	CA-21	SDL - 4	Controls aanwezig in ISO control mapping / NIST raamwerk Scheiding van omgevingen niet expliciet benoemd. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. Hieruit is op te maken dat Microsoft de ontwikkel-, test- en productieomgevingen voor M365 scheidt om de risico's van ongeautoriseerde toegang of wijzigingen in de productieomgeving te verminderen.	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het volgen van een Secure Development Lifecycle-methodologie voor haar applicaties die zijn ontwikkeld op Azure. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor de kwaliteitsborging van de applicatie voordat deze naar de Azure-productieomgeving wordt gebracht. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het bewaken van de beveiliging van haar applicaties die op Azure zijn ontwikkeld.
12.1.4.1	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.	CA-21	SDL - 4	Controls aanwezig in ISO control mapping / NIST raamwerk In M365 assurance rapportage geen expliciete control aanwezig omtrent testen in separate omgevingen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft scheidt de ontwikkel-, test- en productieomgevingen voor M365 om de risico's van ongeautoriseerde toegang of wijzigingen in de productieomgeving te verminderen. Microsoft analyseert wijzigingen in het M365-informatiesysteem in een aparte		zie 12.1.4

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				testomgeving voordat ze worden geïmplementeerd in een productieomgeving. Dit omvat het zoeken naar beveiligingsproblemen als gevolg van gebreken, zwakheden, incompatibiliteit of opzettelijke kwaadwilligheid. Azure: Azure test en valideert voorgestelde systeemwijzigingen voorafgaand aan implementatie, hetzij in een afzonderlijke testomgeving, hetzij door een server uit productie te verwijderen, wijzigingen aan te brengen, te testen en de server na succesvolle voltooiing weer in productie te brengen. Wanneer het testen en valideren is voltooid, worden de resultaten gedocumenteerd in de relevante tool voor het bijhouden van wijzigingen, ofwel Azure DevOps of Incident Management (IcM), afhankelijk van het team. Hieruit is op te maken dat niet in de productieomgeving wordt getest.		
12.1.4.2	Wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.	CA-21	SDL - 4	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	zie 12.1.4
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.	CA-17 CA-29 CA-45 CA-50	SDL - 6 VM - 3 VM - 4 C5 - 1	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
12.2.1.1	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	CA-17 CA-29 CA-45 CA-50	SDL - 6 VM - 3 VM - 4 C5 - 1	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om vast te stellen of het downloaden van bestanden beheerst en beperkt is op basis van risico en need-of-use. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
12.2.1.2	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.	CA-17 CA-29 CA-45 CA-50	SDL - 6 VM - 3 VM - 4 C5 - 1	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om vast te stellen op welke manier gebruikers voorgelicht worden en wat de inhoud van deze voorlichting is. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
12.2.1.3	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.	CA-17 CA-29 CA-45 CA-50	SDL - 6 VM - 3 VM - 4 C5 - 1	Controls aanwezig in ISO control mapping / NIST raamwerk In Azure rapportage wordt actualiteit van dergelijke software niet expliciet benoemd. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft implementeert detectie-, preventie- en herstelcontroles, gecombineerd met een passend gebruikersbewustzijn, om M365 te beschermen tegen malware. Het gebruik van antivirus- en anti-malwaresoftware is een belangrijk mechanisme voor de bescherming van M365-middelen tegen schadelijke software. De software is ontworpen om de introductie van computervirussen en wormen op de servicesystemen te detecteren en te voorkomen. De software zal ook geïnfecteerde systemen in quarantaine plaatsen en verdere schade voorkomen totdat herstelmaatregelen zijn genomen. Antivirussoftware biedt zowel preventieve als detectiecontrole over schadelijke software en wordt geïnstalleerd als onderdeel van de initiële build van systemen. De anti-malwareconfiguraties zijn ingesteld om kwaadaardige code in quarantaine te plaatsen, automatisch te worden bijgewerkt zodra er nieuwe updates beschikbaar zijn en om ten minste dagelijks op updates te controleren. Azure: het gebruik van anti-malwaresoftware is een belangrijk mechanisme voor de bescherming van Azure-assets tegen schadelijke software. De software detecteert en voorkomt de introductie van computervirussen, malware, rootkits, wormen en andere kwaadaardige software op de servicesystemen. Anti-malwaresoftware biedt zowel preventieve als detectivecontrole over schadelijke software. Goedgekeurde tools zoals System Center Endpoint Protection (SCEP), Microsoft Endpoint Protection (MEP), Microsoft Defender for Endpoint (MDE) en ClamAV worden geïnstalleerd als onderdeel van de initiële build op alle servers, inclusief alle entry- en exitpunten naar het informatiesysteem. Azure werkt beveiligingsmechanismen voor schadelijke code bij voor anti-malwaresoftware, inclusief definities van handtekeningen wanneer er nieuwe releases beschikbaar zijn. Antimalwaresoftware is geconfigureerd om ten minste dagelijks te controleren op updates voor de handtekeningbestanden en deze automatisch dienovereenkomstig bij te werken. Uit bovenstaande is op te maken dat de anti-malwaresoftware ondersteund wordt door periodieke updates waardoor deze actueel blijft.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.2.1.4	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten: (a) Alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen. (b) Bijlagen en downloads vóór gebruik.	CA-17 CA-29 CA-45 CA-50	SDL - 6 VM - 3 VM - 4 C5 - 1	Controls aanwezig in ISO control mapping / NIST raamwerk Het is niet mogelijk om op te maken op de benoemde aspecten onderdeel zijn van de routinematige scans. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: realtime bescherming is ingeschakeld om downloads te scannen, bestands- en programma-activiteit te bewaken en op heuristisch gedrag gebaseerde monitoring uit te voeren. Antivirussoftware biedt zowel preventieve als detectiecontrole over schadelijke software en wordt geïnstalleerd als onderdeel van de initiële build van systemen. Nadat de juiste antivirussoftware is geïnstalleerd, worden de volgende functies centraal beheerd: - Periodieke scans van het bestandssysteem - Automatische scans van de omgeving - Testen, identificeren en corrigeren van valse positieven die door de tool zijn gegenereerd Azure: om de infectie van Azure door malware op draagbare opslagapparaten te voorkomen, volgen Azure-datacenters de Tools and Removable Media Security Procedure in het Datacenter Services Run Book. De procedure geeft aan dat de volgende acties moeten worden ondernomen met USB-drives voor gebruik in de Azure-omgeving: - Formatteer de USB-drives wanneer de drives voor het eerst worden gekocht bij de fabrikant of leverancier, vóór het eerste gebruik of wanneer ze opnieuw worden gebruikt voor een ander hulpmiddel. - Scan een USB-drive die in een door Azure aangewezen gebied moet worden gebruikt op malware, voordat u de drive naar het gebied brengt. - Nadat u een schijf hebt gebruikt in een door Azure aangewezen gebied, moet u de schijf formatteren voordat u het gebied verlaat. De volgende functies worden centraal beheerd door de juiste anti-malwaretool op elk eindpunt voor elk serviceteam: - Periodieke scans minimaal wekelijks - Realtime scans van bestanden wanneer ze worden gedownload, geopend of uitgevoerd Hieruit is op te maken dat voor M365 real-time bescherming aanwezig is voor het scannen van downloads en monitoren van bestand- en programma-activiteit. Voor Azure is uit bovenstaande op te maken dat een procedure aanwezig is om te voorkomen dat malware via draagbare media wordt overgedragen en dat bestanden worden gescand bij downloaden, openen of uitvoeren. Per interview met Microsoft hebben wij vernomen dat het scannen van bestand niet van toepassing is, aangezien binnen Azure alleen sprake is van infrastructuur.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.2.1.5	De malware scan wordt op verschillende omgevingen uitgevoerd, bijv. op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.	CA-17 CA-29 CA-45 CA-50	SDL - 6 VM - 3 VM - 4 C5 - 1	Controls aanwezig in ISO control mapping/NIST raamwerk Het is niet mogelijk om op te maken op welke omgevingen de malware scan wordt uitgevoerd. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Het gebruik van antivirus- en anti-malwaresoftware is een belangrijk mechanisme voor de bescherming van M365-middelen tegen schadelijke software. De software is ontworpen om de introductie van computervirussen en wormen op de servicesystemen te detecteren en te voorkomen. De software zal ook geïnfecteerde systemen in quarantaine plaatsen en verdere schade voorkomen totdat herstelmaatregelen zijn genomen. Antivirussoftware biedt zowel preventieve als detectiecontrole over schadelijke software en wordt geïnstalleerd als onderdeel van de initiële build van systemen. Azure: Servers: Azure maakt gebruik van System Center Endpoint Protection (SCEP), Microsoft Endpoint Protection (MEP), Microsoft Defender for Endpoint (MDE) en ClamAV om schadelijke code te detecteren. Naast op handtekeningen gebaseerde detectiemechanismen, maken deze tools ook gebruik van gedragsbewaking, netwerkinspectie en heuristiek om kwaadaardige code te detecteren die mogelijk wordt gemist door op handtekeningen gebaseerde methoden. Netwerkapparaten: netwerkapparaten bieden geen native ondersteuning voor anti-malwaresoftware, maar worden beschermd door een combinatie van servergebaseerde anti-malwaresoftware en de veilige coderingspraktijken vereist door de Security Development Lifecycle (SDL), configuratiebeheer en -controle, levering ketenprocessen en diepgaande logging en monitoring. Uit bovenstaande is op te maken dat voor Azure onderscheid wordt gemaakt tussen servers en netwerk devices. Voor M365 wordt gesproken over 'the service systems'. Per interview met Microsoft hebben wij vernomen dat scanning plaatsvindt tot aan de (klant)omgeving.		Algemeen - CUEC: De gebruikersorganisatie is verantwoordelijk voor het uitvoeren van malware scans op alle omgevingen die zij relevant beschouwt.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
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.	CA-50 CA-51	DS - 5 DS - 7 DS - 8 DS - 9 DS - 13 *OPS-08*	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het maken van back-ups van hun gegevens van Azure naar lokale opslag bij beëindiging van het Azure-abonnement. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het bepalen van de configuraties die op hun VM's moeten worden ingeschakeld.
12.3.1.1	Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld.	CA-50 CA-51	DS - 5 DS - 7 DS - 8 DS - 9 DS - 13 *OPS-08*	Controls aanwezig in ISO control mapping / NIST raamwerk Het is niet mogelijk om op te maken of er een beleid is voor het maken van back-ups met daarin eisen voor het bewaren en beschermen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft gebruikt datacenterreplicatieoplossingen voor M365. Elk van de toepasselijke Business Continuity Plans beschrijft de procedures die gelden voor de replicatie van M365-gegevens. Gegevens voor toepassingen en ondersteuningsservices worden gerepliceerd voor redundantie, hoge beschikbaarheid en noodherstel. Gegevensreplicatie vindt plaats binnen hetzelfde datacenter en naar een of meer geografisch verspreide datacenters. De typische configuratie voor replicatie is één primaire server, die binnen hetzelfde datacenter wordt gerepliceerd naar een secundaire server en wordt gerepliceerd over de geografisch verspreide datacenters. Over het algemeen worden de primaire servergegevens gerepliceerd naar drie andere servers met drie andere kopieën. Meerdere kopieën worden in realtime gerepliceerd en andere kopieën hebben een korte, opzettelijke vertraging. Op een gegeven moment zijn gegevens toegankelijk via (1) de primaire server; (2) een secundaire server met realtime gerepliceerde gegevens binnen hetzelfde datacenter waar de primaire server zich bevindt; (3) een secundaire server met realtime gerepliceerde gegevens in een geografisch verspreid datacenter; of (4) een server met een vertraging van		Zie 12.3.1

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				enkele minuten gerepliceerd naar een geografisch verspreid datacenter. Aangezien gegevens toegankelijk zijn voor redundantie, hoge beschikbaarheid of noodherstel voor toepassingen en ondersteuningsservices via het hierboven beschreven gegevensreplicatieproces, wordt gegevensback-up alleen uitgevoerd op specifieke toepassingen om te voldoen aan de vereisten van de Service Level Agreement. Azure: voor informatie op gebruikersniveau die is opgeslagen in Azure Storage, worden gegevens synchroon lokaal gerepliceerd met behulp van Locally Redundant Storage (LRS), die redundantie biedt die gelijk is aan drie exemplaren. Bovendien worden gegevens asynchroon gerepliceerd naar een afzonderlijk datacenter in de zone of naar een externe regio voor accounts die Zone-Redundant Storage (ZRS), Geo-Redundant Storage (GRS) of Read-Access Geo-Redundant Storage (RA) hebben geconfigureerd. -GRS). De back-ups die naar Azure Storage worden verzonden, worden versleuteld met FIPS 140-2-compatibele AES 256-bits versleuteling. Er zijn drie soorten back-ups: Customer Machine, Disk Pod en Tape. Voor back-ups van Customer Machine en Disk Pod worden de gegevens op een locatie aan elkaar gekoppeld en zeven (7) dagen bewaard. Disk Pods maken een back-up naar Blob-opslag, waarin zich twee accounts bevinden, zodat er een back-up van gegevens wordt gemaakt in twee accounts in verschillende regio's. Voor back-up op tape beschrijven het beleid en de procedures van Data Protection Services (DPS) de rollen, verantwoordelijkheden en services voor de back-upstandaarden, het bewaarbeleid, de controle en de rapporten die beschikbaar zijn voor klanten. Alle informatie waarvan een back-up wordt gemaakt en wordt opgeslagen, maakt gebruik van de gegevenstypeclassificatie volgens CELA-gegevensclassificatie. Serviceteams moeten de gegevenstypeclassificatie identificeren die op zijn beurt het toegewezen retentie- en opslagbeleid aanstuurt. Uit bovenstaande blijkt dat voor M365 Business Continuity Plans aanwezig zijn waarin eisen zijn gesteld aan bewaren en beschermen, en voor Azure is op te maken dat backups worden ingericht conform de CELA Data Classification.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.3.1.2	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	CA-50 CA-51	DS - 5 DS - 7 DS - 8 DS - 9 DS - 13 *OPS-08*	Ontbreken control in SOC geaccepteerd door werkgroep. Voor Azure Het is niet mogelijk om op te maken of een expliciete risicoafweging is uitgevoerd om deze punten te bepalen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft stelt, documenteert, implementeert en onderhoudt processen, procedures en controles om het vereiste niveau van continuïteit voor informatiebeveiliging te waarborgen tijdens een ongunstige situatie. Microsoft ontwikkelt een noodplan voor het informatiesysteem dat hersteldoelstellingen, herstelprioriteiten en metrische gegevens biedt. Plannen worden ontwikkeld en onderhouden volgens best practices uit de branche om een afspiegeling te zijn van de huidige productieomgeving. Zie Servicecontinuïteit (https://technet.microsoft.com/en-us/library/office-365-service-continuity.aspx) voor meer informatie. Microsoft handhaaft een raamwerk dat consistent is met best practices in de branche en dat het continuïteitsprogramma op niveaus stimuleert. Het raamwerk omvat: [....] Recovery Time Objectives en Recovery Point Objectives; Continuïteitsplannen met gedocumenteerde procedures [...]. Azure: Azure stelt hersteltijddoelstellingen (RTO) vast voor alle Azure-services en documenteert deze RTO's als onderdeel van het BCM-proces. Essentiële diensten worden gedefinieerd als diensten met een RTO van 168 uur of minder. Door de volledig redundante architectuur van Azure zoals beschreven in de BCP en DRP, zijn alternatieve storage sites in de vorm van Azure datacenters ontworpen en geïmplementeerd om continu beschikbaar te zijn. De beschikbaarheid van de site heeft geen invloed op de RTO of RPO voor een bepaalde Azure-service vanwege de redundante architectuur. Het BCDR-programma in de Azure Global Portal dekt expliciet de bedrijfsprocessen die zijn gedefinieerd tijdens de BIA met Recovery Time Objectives (RTO) en Recovery Point Objectives (RPO) voor elke service. Uit bovenstaande is op te maken dat het maximale toegestane dataverlies en maximale hersteltijd zijn bepaald. Hierbij is echter niet op te maken dat dit op basis van een expliciete risico-afweging heeft plaatsgevonden. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien gebruikersorganisaties zelf verantwoordelijk zijn voor het bepalen van het maximaal toegestane dataverlies en de maximale hersteltijd na een incident.		Algemeen - CUEC: Gebruikersorganisaties zijn verantwoordelijk voor het bepalen van het maximaal toegestane dataverlies en de maximale hersteltijd na een incident.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
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.	CA-50 CA-51	DS - 5 DS - 7 DS - 8 DS - 9 DS - 13 *OPS-08*	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om vast te stellen op basis van de assurance rapportages. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		Zie 12.3.1
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.	CA-50 CA-51	DS - 5 DS - 7 DS - 8 DS - 9 DS - 13 *OPS-08*	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Zie 12.3.1
12.3.1.5	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.	CA-50 CA-51	DS - 5 DS - 7 DS - 8 DS - 9 DS - 13 *OPS-08*	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Zie 12.3.1

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.4.1	Gebeurtenissen registreren: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	CA-48 CA-57 CA-60	SDL -5 VM - 1 VM - 2 VM - 4 VM - 9 VM - 10 VM - 12 C5 - 6 C5 - 7 CCM - 1 CCM - 3 OA - 16 C5 - 1 IM - 1 IM - 2 IM - 3	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.4.1.1	Een logregel bevat minimaal: (a) de gebeurtenis; (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handeling; (e) een datum en tijdstip van de gebeurtenis.	CA-48 CA-57 CA-60	SDL -5 VM - 1 VM - 2 VM - 4 VM - 9 VM - 10 VM - 12 C5 - 6 C5 - 7 CCM - 1 CCM - 3 OA - 16 C5 - 1 IM - 1 IM - 2 IM - 3	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om vast te stellen of alle aspecten zoals beschreven zijn geïmplementeerd. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
12.4.1.2	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	CA-48 CA-57 CA-60	SDL -5 VM - 1 VM - 2 VM - 4 VM - 9 VM - 10 VM - 12 C5 - 6 C5 - 7 CCM - 1 CCM - 3 OA - 16 C5 - 1 IM - 1 IM - 2 IM - 3	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om vast te stellen dat logregels geen gegevens bevatten die tot het doorbreken van de beveiliging kunnen leiden. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.4.1.3	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	CA-48 CA-57 CA-60	SDL -5 VM - 1 VM - 2 VM - 4 VM - 9 VM - 10 VM - 12 C5 - 6 C5 - 7 CCM - 1 CCM - 3 OA - 16 C5 - 1 IM - 1 IM - 2 IM - 3	Controls aanwezig in FedRAMP-raamwerk Voor M365 wordt niet expliciet gesproken over een SOC en/of SIEM. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft produceert, bewaart en beoordeelt regelmatig gebeurtenislogboeken waarin gebruikersactiviteiten, uitzonderingen, fouten en informatiebeveiligingsgebeurtenissen van M365 worden vastgelegd. Het M365 Security Service Engineering-team heeft een algemene set van controleerbare gebeurtenissen ontwikkeld, specifiek voor M365 op basis van doorlopende risicobeoordelingen van het systeem, waarin geïdentificeerde kwetsbaarheden, zakelijke vereisten en M365-beveiligingsnormen zijn verwerkt. De algemene gebeurtenissen worden beoordeeld door het juiste beveiligingsteam wanneer een belangrijke wijziging in het systeem wordt aangebracht om ervoor te zorgen dat eventuele kwetsbaarheden worden aangepakt door de reeks controleerbare gebeurtenissen. Nieuwe gebeurtenissen kunnen worden opgenomen wanneer een nieuwe service online wordt gebracht of wanneer een kwetsbaarheid of bedreiging wordt geïdentificeerd (bijvoorbeeld door middel van beveiligingsbeoordelingen of beveiligingsbulletins) Azure: voor alle hosts in Azure is logboekregistratie van gebeurtenissen ingeschakeld. Als deze functionaliteit is uitgeschakeld of niet succesvol is, wordt een waarschuwing gegenereerd via Geneva Monitoring en wordt de waarschuwing onderzocht als een beveiligingsincident. Activa worden elk geconfigureerd met een Event Forwarding Tool. De Event Forwarding Tool stuurt auditrecords naar de Security Incident and Event Management Tool via een infrastructuur voor het verzamelen van gebeurtenissen die ook beveiligingsgebeurtenissen in de omgeving archiveert. Dit doorsturen van gebeurtenissen vindt in realtime plaats voor het onderling verbonden systeem. Bovendien is antivirussoftware geconfigureerd om bestanden die in het systeem binnenkomen in realtime te scannen en deze in quarantaine te plaatsen als wordt vastgesteld dat ze kwaadaardig zijn. Waarschuwingen van klanten worden vastgelegd in de antivirussoftwaredatabase en de waarschuwingen voor malware-gerelateerde gebeurtenissen worden op drie manieren in bijna realtime naar het Security Response Team gestuurd. Dit gebeurt via waarschuwingen/tickets, e-mails naar het Security Response Team en een feed naar de tool voor beveiligingsincidenten en evenementen. Uit bovenstaande is op te maken dat event logs aanwezig zijn voor M365 en dat deze gebaseerd zijn op risico-inschattingen. Hierbij wordt echter niet gesproken over monitoring door een SOC of SIEM. Voor Azure is uit bovenstaande op te maken dat event logging aanwezig is en dat gebruik wordt gemaakt van een SIEM tool. Hierbij is echter niet op te maken of dit gebaseerd is op een risico-inschatting.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor M365 op te maken dat gebruik wordt gemaakt van een SOC en SIEM. Dit is opgenomen onder SC-22 en IR-4 in de M365 FedRAMP-rapportage. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor Azure op te maken dat logging is opgenomen in de Microsoft Security Program Policy (MSPP). Deze policy wordt beoordeeld door de Microsoft Information Risk Management Council (IRMC), waaruit op te maken is dat hierbij gebruik wordt gemaakt van risicoinschattingen. Dit is opgenomen onder AU-01 in de Azure FedRAMP-rapportage.		
12.4.1.4	Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	CA-48 CA-57 CA-60	SDL -5 VM - 1 VM - 2 VM - 4 VM - 9 VM - 10 VM - 12 C5 - 6 C5 - 7 CCM - 1 CCM - 3 OA - 16 C5 - 1 IM - 1 IM - 2 IM - 3	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om op te maken dat de dreigingen gedeeld worden met NCSC of CERT. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: M365 werkt samen met het Microsoft Trustworthy Computing Team om contacten te onderhouden met externe partijen zoals regelgevende instanties, serviceproviders en brancheorganisaties, zoals het United States Computer Emergency Readiness Team (US-CERT) om ervoor te zorgen dat passende actie kan worden ondernomen en waar nodig advies ingewonnen. M365 vertrouwt op de wereldwijde criminele compliance- en Corporate, External and Legal Affairs (CELA)-teams van Microsoft voor contacten met wetshandhavingsinstanties. Rollen en verantwoordelijkheden voor het beheren en onderhouden van deze relaties zijn vastgelegd. Azure: het Security Response Team identificeert informatie die geschikt is om te correleren en te delen met andere incidentafhandelingsteams voor direct getroffen klanten om een breder perspectief op incidentbewustzijn te krijgen. Het Threat Intelligence Team (MSTIC) van Microsoft coördineert met andere externe organisaties om deze informatie te correleren en te delen. Microsoft gebruikt ook het MSRC Ecosystem Strategy overheidsbeveiligingsprogramma om te coördineren met US-CERT en andere computerbeveiligingsincidentresponsteams (CSIRT's) op nationaal niveau. Microsoft coördineert en maakt gebruik van verschillende bronnen voor incidentbewustzijn, zoals US-Cert/DoD Cert, MSRC, Adobe, Cisco, CVE en Qualys. Het Azure Security Response Team brengt een directe, samenwerkingsrelatie tot stand tussen externe providers zoals US-CERT, DoD-CERT en IC-CERT, die het Security Response Team bruikbare informatie kunnen sturen om te helpen beschermen, bewaken, analyseren, detecteren en reageren op ongeoorloofde activiteit. Uit bovenstaande is op te maken dat contacten worden onderhouden met externe partijen, waaronder de US-CERT. Tevens is hieruit op te maken dat dit een coöperatieve relatie betreft, en dat in geval van incidenten melding wordt gemaakt. Echter is hierbij niet expliciet op te		Algemeen - CUEC: Security dreigingen worden door Microsoft in het platform met klanten gedeeld. De gebruikersorganisatie is zelf verantwoordelijk voor het delen met relevante instanties wanneer nodig.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				maken dat ook in geval van nieuwe dreigingen (i.t.t. incidenten) ook melding wordt gemaakt. Per interview met Microsoft hebben wij vernomen dat dreigingen op de continuïteit worden gemeld bij de Ierse toezichthouder. Microsoft is daarnaast in contact met NCSC omtrent threat intelligence. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien uit aanvullende informatie blijkt dat contacten met NCSC en CERT worden onderhouden. Tevens is de gebruikersorganisatie zelf verantwoordelijk voor het delen met relevante instanties wanneer nodig.		
12.4.1.5	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	CA-48 CA-57 CA-60	SDL -5 VM - 1 VM - 2 VM - 4 VM - 9 VM - 10 VM - 12 C5 - 6 C5 - 7 CCM - 1 CCM - 3 OA - 16 C5 - 1 IM - 1 IM - 2 IM - 3	Ontbreken control in SOC geaccepteerd door werkgroep. Voor M365 wordt niet expliciet gesproken over een SOC en/of SIEM. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Azure: voor alle hosts in Azure is event logging ingeschakeld. Als deze functionaliteit is uitgeschakeld of niet succesvol is, wordt een waarschuwing gegenereerd via Geneva Monitoring en wordt de waarschuwing onderzocht als een beveiligingsincident. Activa worden elk geconfigureerd met een Event Forwarding Tool. Azure houdt gebeurtenissen en incidenten bij via het Incident Management-systeem (IcM) en Service Now (SNow) en maakt gebruik van Azure Security Monitoring (ASM) en SCUBA binnen de omgeving ter ondersteuning van het incidentbeheerproces. Deze systemen maken gebruik van geautomatiseerde mechanismen om incidenten te identificeren en om incidenten te documenteren, te volgen en te rapporteren. Interne webpagina's en Standard Operation Procedures (SOP's) bieden advies en assistentie aan het personeel van het serviceteam voor het afhandelen en rapporteren van beveiligingsincidenten, waaronder de Azure Incident Management SOP en de service -team specifieke SOP's voor incidentbeheer. Voor M365 wordt niet gesproken over monitoring door een SOC of SIEM. Voor Azure is uit bovenstaande op te maken dat event logging aanwezig is en dat gebruik wordt gemaakt van een SIEM tool. Tevens is informatie over het rapporteren van security incidenten opgenomen in SOPs. Hierbij is echter niet af te leiden of heldere regels voor SOC/SIEM aanwezig zijn wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor M365 op te maken dat gebruik wordt gemaakt van een SOC en SIEM. Dit is opgenomen onder SC-22 en IR-4 in de M365 FedRAMP-rapportage. Uit ontvangen FedRAMP-rapportages is op te maken dat interne richtlijnen aanwezig zijn voor		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				betrekken van, escaleren naar of rapporteren aan verschillende partijen binnen de organisatie. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien het aantonen van deze maatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.4.2	Beschermen van informatie in logbestanden: Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	n.v.t.	CCM - 3	Controls aanwezig in FedRAMP-raamwerk In de assurance rapportage is de bescherming van informatie in logbestanden niet expliciet opgenomen. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is op te maken dat alleen beheerders van M365-serviceteams toegang hebben tot security logs. Als een beheerder van een serviceteam loggegevens lokaal verwijdert, wordt deze activiteit vastgelegd en wordt er een waarschuwing gegenereerd. Audit-informatie die EUII en klantinhoud bevat, is gehasht en/of versleuteld en kan alleen worden gelezen als een geautoriseerde gebruiker toegang heeft via M365. Geautoriseerde M365-medewerkers kunnen alleen informatie lezen die is opgeslagen in de repositoryservice en krijgen geen toestemming om logs te wijzigen of te verwijderen. Auditinformatie die PII bevat, wordt verwijderd voordat deze naar een opslagplaats voor audit logs wordt verzonden. Audit-informatie wordt tijdens het transport versleuteld en opgeslagen in een versleutelde opslagplaats. Dit is opgenomen onder AU-9 in de M365 FedRAMP-rapportage.	Controls aanwezig in assurance rapportage (SOC)	
12.4.2.1	Er is een overzicht van logbestanden die worden gegenereerd.	n.v.t.	CCM - 3	Controls aanwezig in FedRAMP-raamwerk Overzicht van logbestanden staat niet beschreven in M365 en Azure rapportage. Hiervoor is		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft beschermt M365-faciliteiten en loggegevens tegen manipulatie en ongeautoriseerde toegang. Auditgegevens worden voortdurend geanalyseerd op indicaties van ongepaste of ongebruikelijke activiteiten met behulp van een formeel monitoringproces. Bevindingen worden gerapporteerd met behulp van een responsproces voor beveiligingsincidenten. De veronderstelde inbreukhouding van Microsoft omvat het controleren van de toegang en acties van de operator (beheerder). Azure: Azure implementeert het genereren van audits door alle servers, netwerkapparaten en services zo te configureren dat ze de mogelijkheid hebben om auditrecords en metagegevens van auditrecords te genereren. Uit bovenstaande informatie is voor M365 en Azure niet op te maken of een overzicht van logbestanden aanwezig is. Uit aanvullende ontvangen FedRAMP-rapportages (geen assurance) is op te maken dat voor M365 een overzicht aanwezig is van alle events die gelogd moeten worden, evenals dat dit het M365 Securityteam voor alle servers specificeert welke events onderzocht moeten worden. Dit is opgenomen onder AU-2 in de M365 FedRAMP-rapportage. Voor Azure is uit de FedRAMP-rapportages op te maken dat sets van events zijn gedefinieerd op basis van doorlopende risico-inschattingen. Dit is opgenomen onder AU-02 in de Azure FedRAMP-rapportage.		
12.4.2.2	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	n.v.t.	CCM - 3	Controls aanwezig in FedRAMP-raamwerk Bewaarperiode van logging staat niet beschreven in M365 rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: activa die eigendom zijn van M365, inclusief beveiligingsdocumenten, worden waar nodig bewaard op basis van de bewaarvereisten die zijn vastgesteld door het M365-informatiebeveiligingsbeleid. Azure: Azure bewaart verzamelde logs in de opslag gedurende ten minste negentig (90) dagen ter ondersteuning van onderzoeken naar beveiligingsincidenten en om te voldoen aan wettelijke bewaarvereisten. Azure slaat auditlogboeken offline op voor ten minste één (1) jaar binnen Kusto-opslag. C+AI Security heeft een archiveringsinfrastructuur ontwikkeld om auditrecords veilig op te slaan op servers die bestemd zijn voor archiveringsdoeleinden. De servers zijn ontworpen om de integriteit van gearchiveerde bestanden te verifiëren en stellen geautoriseerde gebruikers in staat om naar een archieflocatie te bladeren. Auditrecords worden opgeslagen op gecentraliseerde logservers die zijn beveiligd tegen wijziging.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				Uit bovenstaande is voor Azure niet op te maken dat de bewaarperiode is bepaald op basis van een expliciete risico-afweging. Voor M365 is niet op te maken wat de bewaarperiode is en hoe deze is bepaald. Uit aanvullende ontvangen FedRAMP-rapportages (geen assurance) is voor M365 en Azure op te maken dat audit log informatie minstens één jaar wordt bewaard. Dit is opgenomen onder AU-11 in de M365 en Azure FedRAMP-rapportages.		
12.4.2.3	Er is een (onafhankelijke) interne audit procedure die minimaal halfjaarlijks toetst op het ongewijzigd bestaan van logbestanden.	n.v.t.	CCM - 3	Geen controls beschreven Interne audit procedure die minimaal halfjaarlijks toetst op het ongewijzigd bestaan van logbestanden staat niet beschreven in M365 en Azure rapportage of aanvullende stukken.		
12.4.2.4	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.	n.v.t.	CCM - 3	Controls aanwezig in ISO control mapping / NIST raamwerk Dit staat niet specifiek beschreven in M365 en Azure rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft beschermt M365-faciliteiten en loggegevens tegen manipulatie en ongeautoriseerde toegang. Auditgegevens worden voortdurend geanalyseerd op indicaties van ongepaste of ongebruikelijke activiteiten met behulp van een formeel monitoringproces. Bevindingen worden gerapporteerd met behulp van een responsproces voor beveiligingsincidenten. De veronderstelde inbreukhouding van Microsoft omvat het controleren van de toegang en acties van de operator (beheerder). Azure: schadelijke activiteiten op het activum die de verzameling van beveiligingslogboeken proberen te beïnvloeden, worden gecontroleerd en gewaarschuwd, inclusief bewaking voor het wissen van het logboek voor beveiligingsgebeurtenissen en wijzigingen in het auditbeleid. Uit bovenstaande is op te maken dat zowel voor M365 als Azure maatregelen zijn ingericht om te voorkomen dat loggegevens gewijzigd of verwijderd worden. Daarnaast is op te maken dat pogingen daartoe worden gemonitord en hiervoor alerts zijn ingericht. Hierbij is voor Azure echter niet op te maken of dit via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16 verloopt. Per interview met Microsoft hebben wij vernomen dat binnen Azure andere tooling gebruikt wordt, maar het proces verder overeenkomt met het proces zoals doorlopen wordt voor M365.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.4.3	Logbestanden van beheerders en operators: Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	CA-57 CA-60	VM - 2 CCM - 3	Controls aanwezig in ISO control mapping / NIST raamwerk Het vastleggen en beoordelen van dergelijke logbestanden is niet expliciet beschreven in de assurance rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. Hieruit is op te maken dat M365 de activiteiten van systeembeheerders en systeemoperators registreert, de logs zijn beveiligd en regelmatig worden gecontroleerd.	Controls aanwezig in FedRAMP-raamwerk Het vastleggen en beoordelen van dergelijke logbestanden is niet expliciet beschreven in de assurance rapportage. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor Azure op te maken dat onder de audit events ook 'privilege functions' en (voor webapplicaties) alle administrator activiteiten worden gelogd. Dit is opgenomen onder AU-02 in de Azure FedRAMP-rapportage.	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.4.4	Kloksynchronisatie: De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	n.v.t.	CCM - 4	Controls aanwezig in ISO control mapping / NIST raamwerk Kloksynchronisatie is niet expliciet beschreven in de assurance rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. Microsoft synchroniseert de klokken van relevante informatieverwerkingssystemen binnen een organisatie of beveiligingsdomein met één referentietijdbron. Microsoft registreert tijdstempels voor auditrecords die kunnen worden toegewezen aan Coordinated Universal Time (UTC) of Greenwich Mean Time (GMT). Auditrecords en gebeurtenissen die door M365-servers worden gegenereerd, worden vastgelegd met tijdstempels. Servers zijn geconfigureerd om interne klokken te synchroniseren met Active Directory-domeincontrollers met behulp van het Network Time Protocol NTP). Servers zijn gekoppeld aan een Active Directory-domein en geconfigureerd om ten minste elk uur geverifieerde tijdupdates te ontvangen van een lokale domeincontroller met behulp van NTP. Uit bovenstaande is op te maken dat kloksynchronisatie wordt toegepast.	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.5.1	Software installeren op operationele systemen: Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	CA-18 CA-21 CA-38 CA-46	CM - 2 CM - 4 CM - 5 CM - 10 CM - 13	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
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 maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.	CA-24 CA-27 CA-45 ELC-09	VM - 4 VM - 6 VM - 13 BC - 7	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het beoordelen van openbare Azure-beveiligings- en patchupdates. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het toepassen van patches indien zij niet is aangemeld voor automatische upgrades. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het verifiëren van de beveiliging van patching en het onderhouden van applicaties en/of componenten van derden die ze installeren op de Azure-productieomgeving.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
						M365 - CUEC-06: De gebruikersorganisatie is verantwoordelijk voor het beveiligen van de software en hardware die worden gebruikt om toegang te krijgen tot M365.
12.6.1.1	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC-classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.	CA-24 CA-27 CA-45 ELC-09	VM - 4 VM - 6 VM - 13 BC - 7	Ontbreken control in SOC geaccepteerd door werkgroep. Uit de rapportages Het is niet mogelijk om op te maken of patches uiterlijk binnen een week geïnstalleerd worden, en of in tussentijd op basis van een expliciete risicoafweging mitigerende maatregelen getroffen worden. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft verkrijgt tijdig informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt door middel van dagelijkse kwetsbaarheidsscans. De blootstelling van Microsoft aan dergelijke kwetsbaarheden wordt geëvalueerd en er worden passende maatregelen genomen om het bijbehorende risico aan te pakken. Microsoft identificeert, rapporteert en corrigeert fouten in informatiesystemen via kwetsbaarheidsbeheer, incidentresponsbeheer en patch- en configuratiebeheerprocessen. Azure: om het risico van blootstelling aan bekende beveiligingsproblemen te voorkomen, is het de verantwoordelijkheid van elke Asset Owner om ervoor te zorgen dat hun systemen over de nieuwste beveiliging gerelateerde patches beschikken. De meeste beveiligingsupdates moeten binnen dertig (30) dagen na de kennisgeving van de beschikbaarheid van de update worden geïnstalleerd. Azure voert een analyse uit op de lijst met beveiligingsrichtlijnen die door het C+AI-beveiligingsteam zijn verstrekt om de toepasbaarheid op Azure-assets te bevestigen. Na voltooiing van de analyse stellen de Azure-serviceteams de laatste maandelijkse patchlijst op waarin de kwetsbaarheden worden gespecificeerd die moeten worden gepatcht. Beveiligingsherstel wordt als volgt geïmplementeerd: - Remediëring voor kwetsbaarheden met een hoog risico wordt geïmplementeerd binnen dertig (30) dagen nadat de kwetsbaarheidsbeperking door de leverancier is vrijgegeven. - Remediëring van kwetsbaarheden met gemiddeld risico wordt geïmplementeerd binnen negentig (90) dagen nadat de kwetsbaarheid door de leverancier is vrijgegeven. - Kwetsbaarheden met laag risico worden beoordeeld door Azure Security. Veel		Zie 12.6.1 In aanvulling heeft de werkgroep aangegeven dat het (afhankelijk van de afgenomen dienstverlening: IaaS, PaaS of SaaS) voor zowel de gebruikersorganisatie (eindgebruiker) als de tenantbeheerder (SSC-ICT) van belang is na te gaan op welke gebieden zij patches kunnen installeren c.q. instellingen hiervoor kunnen configureren.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				scanresultaten met laag risico worden door Azure Security bepaald om geen risico te vormen voor Azure. In dit geval wordt een uitzondering ingediend en wordt het resultaat niet hersteld. Als wordt vastgesteld dat het resultaat een risico vormt voor Azure, wordt herstel binnen honderdtachtig (180) dagen geïmplementeerd. Azure Security verifieert de mate van naleving met behulp van kwetsbaarheidsscanners die in Azure zijn geïmplementeerd. Uit bovenstaande is op te maken dat voor Azure binnen 30 dagen opvolging gegeven moet worden aan 'high risk vulnerabilities'. Dit is niet in lijn met de overheidsmaatregel. Voor M365 is niet op te maken binnen welke termijn patches voor 'high risk vulnerabilities' geïnstalleerd moeten worden. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor M365 op te maken dat patches voor 'high risk vulnerabilities' binnen 30 dagen geïnstalleerd moeten worden. Dit is opgenomen onder SI-2 in de M365 FedRAMP-rapportage. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien het aantonen van deze maatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
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.	CA-26 CA-27 CA-38 CA-45 CA-46 CA-47 CA-48 *CC6.8*	OA - 1 CM - 12 PE - 1 SOC2 - 15 ED - 1 ED - 3 *CCC-04*	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	M365 - CUEC-06: De gebruikersorganisatie is verantwoordelijk voor het beveiligen van de software en hardware die worden gebruikt om toegang te krijgen tot M365.
12.6.2.1	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).	CA-26 CA-27 CA-38 CA-45 CA-46 CA-47 CA-48 *CC6.8*	OA - 1 CM - 12 PE - 1 SOC2 - 15 ED - 1 ED - 3 *CCC-04*	Ontbreken control in SOC geaccepteerd door werkgroep. Wordt niet expliciet benoemd in controls in Azure- en M365-assurance rapportages. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		Zie 12.6.2

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen: Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	ELC-11	SOC2 - 20	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
13.1.1	Beheersmaatregelen voor netwerken: Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	CA-39 CA-40 CA-41 CA-48	VM - 1 VM - 3 VM - 4 VM - 6 VM - 9 OA - 16 OA - 18	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	M365 - CUEC-04: De gebruikersorganisaties is verantwoordelijk voor het afdwingen van het gewenste versleutelingsniveau voor netwerk-sessies.
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
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.	ELC-15	SOC2 - 25 VM - 3 VM - 9 OA - 16	Controls aanwezig in ISO control mapping / NIST raamwerk In assurance rapportages wordt niet expliciet gesproken over het opnemen van alle genoemde onderwerpen in de control omtrent beveiliging van netwerkdiensten in overeenkomsten betreffende netwerkdiensten. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Hieruit is onder andere op te maken dat verschillende maatregelen zijn getrokken om het dataverkeer dat de organisatie binnenkomt of uitgaan te bewaken (zie 13.1.2.1).		M365 - CUEC-04: De gebruikersorganisaties is verantwoordelijk voor het afdwingen van het gewenste versleutelingsniveau voor netwerk-sessies.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
13.1.2.1	Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	ELC-15	SOC2 - 25 VM - 3 VM - 9 OA - 16	Controls aanwezig in ISO control mapping / NIST raamwerk Uit assurance rapportages van Azure en M365 niet op te maken dat het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen). Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Er worden meerdere technieken gebruikt om informatiestromen te beheersen, inclusief maar niet beperkt tot protocolbeperkingen: verkeer van en naar klanten wordt verzonden via versleutelde verbindingen. Microsoft implementeert grensbescherming door het gebruik van gecontroleerde apparaten aan de netwerkgrens en op belangrijke punten binnen het netwerk. Microsoft implementeert informatiestroomcontrole door alleen verbindingen en communicatie toe te staan die nodig zijn om het systeem mogelijk te maken, door standaard andere poorten, protocollen en verbindingen te blokkeren, zoals gedefinieerd in de Microsoft Online Services-beveiligingsstandaard. M365 gebruikt FIPS 140-2 Level 2-gevalideerde versleutelingen voor verbindingen van klanten, derden en externe toegang tot de accreditatiegrens. M365-ondersteuningspersoneel gebruikt FIPS 140-2-gevalideerde TLS-codering voor verbindingen die buiten de grens van M365 reiken. Microsoft produceert, bewaart en beoordeelt regelmatig gebeurtenislogboeken waarin (o.a.) informatiebeveiligingsgebeurtenissen van M365 worden vastgelegd. Het M365 Security Service Engineering-team heeft een algemene reeks controleerbare gebeurtenissen ontwikkeld, specifiek voor M365. [Dit omvat …] tickets of bijbehorende automatisch gegenereerde e-mails die zijn verzonden naar verschillende M365-teams, op basis van verkeers- of systeemgebeurtenissen en vastgesteld dat de statistische patroonanalysemetingen worden gebruikt om ongepaste of ongebruikelijke activiteit te detecteren. Azure: Azure implementeert grensbeveiliging via een diepgaande verdedigingsstrategie. Als een cloudservice die bestaat uit talloze serviceteams en klanten, zijn logische isolatie en segmentatie van cruciaal belang voor de veilige operaties van Azure. De strategie omvat netwerksegmentatie via VLAN- en Network Security Group (NSG)-segmentatie, ACL-beperkingen en versleutelde communicatie. Azure maakt alleen verbinding met externe netwerken of informatiesystemen via de beheerde netwerken en Edge Routers van Azure Networking. De netwerkinterfaces bieden grensbeveiliging op het Edge Router-netwerkniveau en zijn ingericht volgens de Microsoft- en Azure-beveiligingsarchitecturen. Aanvullende maatregelen om Azure-informatiesystemen te beschermen tegen kwaadwillende activiteiten zijn onder meer; Software load balancers, Non-routable IP addressing, Packet filtering,Host-based firewalls,VLAN and NSG isolation, Jumpboxes, Debug Servers, Hop Boxes en VPNs. Al het verkeer op de (netwerk) grens is beperkt tot geautoriseerde verbindingen zoals		Zie 13.1.2

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				gedefinieerd door het serviceteam. Uit bovenstaande is op te maken dat verschillende maatregelen zijn getroffen om het dataverkeer dat de organisatie binnenkomt of uitgaan te bewaken.		
13.1.2.2	Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).	ELC-15	SOC2 - 25 VM - 3 VM - 9 OA - 16	Ontbreken control in SOC geaccepteerd door werkgroep. Uit assurance rapportages van Azure en M365 niet op te maken dat de dreigingen gedeeld worden met NCSC of CERT. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: M365 werkt samen met het Microsoft Trustworthy Computing Team om contacten te onderhouden met externe partijen zoals regelgevende instanties, serviceproviders en brancheorganisaties, zoals het United States Computer Emergency Readiness Team (US-CERT) om ervoor te zorgen dat passende actie kan worden ondernomen en waar nodig advies ingewonnen. M365 vertrouwt op de wereldwijde criminele compliance- en Corporate, External and Legal Affairs (CELA)-teams van Microsoft voor contacten met wetshandhavingsinstanties. Rollen en verantwoordelijkheden voor het beheren en onderhouden van deze relaties zijn vastgelegd. Azure: het Security Response Team identificeert informatie die geschikt is om te correleren en te delen met andere incidentafhandelingsteams voor direct getroffen klanten om een breder perspectief op incidentbewustzijn te krijgen. Het Threat Intelligence Team (MSTIC) van Microsoft coördineert met andere externe organisaties om deze informatie te correleren en te delen. Microsoft gebruikt ook het MSRC Ecosystem Strategy overheidsbeveiligingsprogramma om te coördineren met US-CERT en andere computerbeveiligingsincidentresponsteams (CSIRT's) op nationaal niveau. Microsoft coördineert en maakt gebruik van verschillende bronnen voor incidentbewustzijn, zoals US-Cert/DoD Cert, MSRC, Adobe, Cisco, CVE en Qualys. Het Azure Security Response Team brengt een directe, samenwerkingsrelatie tot stand tussen externe providers zoals US-CERT, DoD-CERT en IC-CERT, die het Security Response Team bruikbare informatie kunnen sturen om te helpen beschermen, bewaken, analyseren, detecteren en reageren op ongeoorloofde activiteit. Uit bovenstaande is op te maken dat contacten worden onderhouden met externe partijen, waaronder de US-CERT. Tevens is hieruit op te maken dat dit een coöperatieve relatie betreft, en dat in geval van incidenten melding wordt gemaakt. Echter is hierbij niet expliciet op te maken dat ook in geval van dreigingen (i.t.t. incidenten) ook melding wordt gemaakt. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien uit aanvullende informatie blijkt dat contacten met NCSC en CERT worden onderhouden.		Zie 13.1.2

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
13.1.2.3	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	n.v.t.	n.v.t.	Ontbreken control in SOC geaccepteerd door werkgroep. Microsoft vraagt niet om inzet advies bij de NBV, wel hebben wij uit informatie (geen assurance) van Microsoft ontvangen waaruit blijkt dat gebruik wordt gemaakt van encryptiemiddelen die voldoen aan de FIPS140-2 standaard. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		Zie 13.1.2 Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het bepalen, implementeren en beheren van versleutelingsvereisten voor haar gegevens binnen het Azure-platform waar Azure dit niet standaard inschakelt en/of dit door de gebruikersorganisatie kan worden beheerd.
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.	ELC-15	SOC2 - 25 VM - 3 VM - 9 OA - 16	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Zie 13.1.2

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
13.1.3	Scheiding in netwerken: Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.	CA-39	OA - 18 DS - 16 LA - 3	Controls aanwezig in ISO control mapping / NIST raamwerk Scheiding van groepen informatiediensten, -gebruikers en -systemen in netwerken niet expliciet opgenomen in assurance rapportages. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Hieruit is op te maken dat M365 tenants van elkaar geïsoleerd worden op basis van aangepaste code en beveiligingsgrenzen, of silo's, die logisch worden afgedwongen via Active Directory. Voor Azure is hieruit op te maken dat logische isolatiemechanismen geïmplementeerd zijn voor het isoleren van de klantomgeving (zie ook 13.1.3.1). Per interview met Microsoft hebben wij vernomen dat Microsoft enkel verantwoordelijk is voor de scheiding op klantniveau (scheiding tussen tenants) en dat klanten zelf verantwoordelijk zijn voor de scheiding binnen hun eigen omgeving(en).		M365 - CUEC-01: De gebruikersorganisaties is verantwoordelijk voor het op de juiste manier autoriseren van gebruikers die toegang krijgen tot de bronnen en het bewaken van de voortdurende geschiktheid van toegang. M365 - CUEC-06: De gebruikersorganisaties is verantwoordelijk voor het beveiligen van de software en hardware die worden gebruikt om toegang te krijgen tot M365.
13.1.3.1	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	CA-39	OA - 18 DS - 16 LA - 3	Controls aanwezig in ISO control mapping / NIST raamwerk Beveiligingsniveaus van gescheiden groepen niet expliciet opgenomen in assurance rapportages. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft scheidt groepen informatiediensten, gebruikers en informatiesystemen op netwerken. M365 scheidt gebruikersfunctionaliteit (inclusief gebruikersinterfaceservices) van functionaliteit voor informatiesysteembeheer. Het primaire principe van netwerkbeveiliging is om alleen verbindingen en communicatie toe te staan die nodig zijn voor de werking van het systeem, waarbij standaard andere poorten, protocollen en verbindingen worden geblokkeerd. De netwerken binnen M365-datacenters zijn ontworpen om meerdere afzonderlijke netwerksegmenten te creëren. Deze segmentatie helpt bij het fysiek scheiden van kritieke back-endservers en opslagapparaten van de openbare interfaces. Gegevensopslag en -verwerking zijn logisch gescheiden tussen klanten van dezelfde service door middel van Active Directory-structuur en -mogelijkheden die speciaal zijn ontwikkeld om		Zie 13.1.3

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				te helpen bij het bouwen, beheren en beveiligen van multi-tenant-omgevingen. De multi-tenant beveiligingsarchitectuur zorgt ervoor dat klantgegevens die zijn opgeslagen in M365-datacenters niet toegankelijk zijn voor of worden aangetast door andere organisaties. Active Directory wordt gebruikt om de ongeoorloofde en onbedoelde informatieoverdracht via gedeelde systeembronnen te controleren en te voorkomen. Tenants worden van elkaar geïsoleerd op basis van aangepaste code en beveiligingsgrenzen, of silo's, die logisch worden afgedwongen via Active Directory. Azure: Azure implementeert meerdere sterke logische isolatiemechanismen voor het isoleren van de klantomgeving, infrastructuurcomponenten en beheerhulpprogramma's, in plaats van fysieke isolatie. Deze mechanismen omvatten: - Virtuele laag 2 op laag 3-routering, die het beheervlak isoleert van het gegevensvlak - VLAN-isolatie, die de Fabric Controller, andere apparaten en zowel interne serviceteams als klanten isoleert - VM en Host OS-code isoleert het Host OS van VM's en van elkaar - Isolatie van opslagaccounts via unieke geheime sleutels De Azure-beveiligingshulpprogramma's, -mechanismen en ondersteuningsonderdelen die zijn gekoppeld aan systeem- en beveiligingsbeheer, zijn logisch geïsoleerd in een afzonderlijk subnet dat bekend staat als de Security Global Infrastructure LAN (GIL). Het Security GIL-subnet van Azure maakt deel uit van het grotere Global Infrastructure LAN, een logisch gescheiden subnet dat wordt beheerd door het Azure Networking-team. Om netwerkverkeer voor het subnet te beperken, worden ACL's gebruikt voor inkomend en uitgaand verkeer. Toegang tot de Security GIL-middelen is beperkt tot alleen goedgekeurde systeembeheerders die smartcards en pincodes gebruiken via Jumpboxes, Network Hop Boxes en Debug Servers. Azure-serviceteams zijn ook logisch van elkaar geïsoleerd vanwege de aard van de Azure-cloud, waarbij dezelfde tenantisolatie wordt gebruikt die door externe klanten wordt gebruikt. Serviceteams worden bij hun gebruik van Azure behandeld als externe klanten. Met uitzondering van het beheervlak en de ondersteunende teams, worden services uitgevoerd binnen standaard Azure-netwerkbeveiligingsgroepen die logisch geïsoleerd zijn van de rest van Azure. Dit zorgt ervoor dat services zoals PKI, Geneva Monitoring, Azure Security Monitoring, Service 360, JIT, Key Vault en meer standaard logisch geïsoleerd zijn. Uit bovenstaande is op te maken dat scheiding in netwerken aanwezig is, echter is hieruit niet expliciet op te maken dat alle gescheiden groepen een gedefinieerd beveiligingsniveau hebben.		
13.2.1	Beleid en procedures voor informatietransport: Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten	CA-36 CA-37 CA-44 CA-45	IS - 1 DS - 2 DS - 3	Controls aanwezig in ISO control mapping / NIST raamwerk Beleid en procedures voor informatietransport niet specifiek opgenomen in assurance	Controls aanwezig in ISO control mapping / NIST raamwerk Beleid en procedures voor informatietransport niet specifiek	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het bepalen,

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
	verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	CA-54 CA-55 CA-62 CA-63 CA-64 *CC6.4* *CC6.7*		rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft de ISO27001-certificering (2016) voor M365. Microsoft heeft formeel beleid, procedures en controles voor overdracht om de overdracht van informatie te beschermen door het gebruik van verschillende soorten communicatiefaciliteiten. Microsoft implementeert grensbeveiliging door het gebruik van gecontroleerde apparaten aan de netwerkgrens en op belangrijke punten binnen het M365-netwerk. Het primaire principe van netwerkbeveiliging is om alleen verbindingen en communicatie toe te staan die nodig zijn voor de werking van het systeem, waarbij standaard andere poorten, protocollen en verbindingen worden geblokkeerd. Toegangscontrolelijsten (ACL's) zijn het geprefereerde mechanisme om netwerkcommunicatie te beperken op basis van bron- en doelnetwerken, protocollen en poortnummers. Goedgekeurde mechanismen om netwerkgebaseerde ACL's te implementeren zijn onder meer: - Gelaagde ACL's op routers beheerd door Microsoft's Cloud Infrastructure & Operations (MCIO)-team - IPsec-beleid toegepast op hosts om communicatie te beperken (indien gebruikt in combinatie met gelaagde ACL's), firewallregels en hostgebaseerde firewallregels M365 gebruikt FIPS 140-2 Level 2-gevalideerde versleutelingen voor verbindingen van klanten, derden en externe toegang tot de M365-accreditatiegrens. M365-ondersteuningspersoneel gebruikt FIPS 140-2-gevalideerde TLS-codering voor verbindingen die buiten de grenzen van M365 vallen. TLS gebruikt cryptografische mechanismen waarmee	opgenomen in assurance rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft het NIST-framework (2021) voor Azure. Azure-services gebruiken altijd beveiligd transport zoals TLS of HTTPS. Versleuteling in transport wordt aangepakt door het transportprotocol. Azure implementeert de transmissie-integriteit en vertrouwelijkheidscontrole door ervoor te zorgen dat cryptografie wordt geïmplementeerd via een hybride model. Azure biedt FIPS 140-2-compatibele versleutelingen die integriteitsvalidatie bevatten voor klantverbindingen, onderling verbonden systeemverbindingen en RAS-verbindingen. Voor verbindingen met klanten is Azure geconfigureerd om te onderhandelen over FIPS-compatibele TLS-protocollen met ondersteunde clientbrowsers, hoewel niet-FIPS-compatibele protocollen worden ondersteund voor ondersteuning van oudere browsers. Verbindingen binnen de accreditatiegrens vinden plaats binnen Azure-faciliteiten. Aangezien Azure eigenaar is van en de toegang tot deze verbindingen beheert, is er geen FIPS 140-2-versleuteling vereist. Service-to-service-communicatie vindt echter plaats via TLS 1.2 en interne communicatie tussen Azure-datacenters wordt verzonden via FIPS 140-2-compatibele AES 256-link-encryptors om de vertrouwelijkheid te waarborgen.	implementeren en beheren van versleutelingsvereisten voor haar gegevens binnen het Azure-platform waar Azure dit niet standaard inschakelt en/of dit door de gebruikersorganisatie kan worden beheerd.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				client-/servertoepassingen via het netwerk kunnen communiceren op een manier die is ontworpen om afluisteren en sabotage te voorkomen. Uit bovenstaande is op te maken dat beleid en procedures voor informatietransport aanwezig zijn.		
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
13.2.2	Overeenkomsten over informatietransport: Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	ELC-15	SOC2 - 3 SOC2 - 25	Controls aanwezig in ISO control mapping / NIST raamwerk Overeenkomsten die betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen zijn niet expliciet opgenomen in assurance rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. De overeenkomsten van Microsoft hebben betrekking op de veilige overdracht van bedrijfsinformatie tussen Microsoft en externe partijen. Microsoft documenteert voor elke interconnectie de interfacekenmerken, beveiligingsvereisten en de aard van de gecommuniceerde informatie. Microsoft vereist dat derden (externe informatiesysteemservices) die betrokken zijn bij M365 een Microsoft Master Vendor Agreement (MMVA) en een Interconnection Security Agreement (ISA) ondertekenen. De MMVA vereist dat de derde partij voldoet aan het toepasselijke M365-beveiligingsbeleid en beveiligingsprocedures implementeert om de openbaarmaking van vertrouwelijke informatie van Microsoft te voorkomen. M365 bevat bepalingen in de MMVA en eventuele bijbehorende Statement of Work	Controls aanwezig in ISO control mapping / NIST raamwerk Overeenkomsten die betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen zijn niet expliciet opgenomen in assurance rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over NIST-framework (2021) voor Azure. Zoals beschreven in het Microsoft Security Program Policy (MSPP) en bijbehorende standaarden, hanteert Azure een deny-all, permit-by-exception-beleid om het Azure-informatiesysteem verbinding te laten maken met externe informatiesystemen. Momenteel heeft Azure geen verbindingen met externe informatiesystemen. De enige verbindingen zijn met interne Microsoft-services. Azure vereist geen ISA's (Interconnection Security Agreements) of MOU's (Memoranda of Understanding) voor interne verbindingen met Microsoft.	M365 - CUEC-04: De gebruikersorganisaties is verantwoordelijk voor het afdwingen van het gewenste versleutelingsniveau voor netwerk-sessies.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				(SOW) waarbij elke leverancier ingaat op de noodzaak om de juiste beveiligingsmaatregelen te gebruiken. Leveranciers die gevoelige gegevens verwerken, moeten voldoen aan de privacy praktijken en gegevensbeschermingsvereisten van Microsoft voor leveranciers. Uit bovenstaande is op te maken dat overeenkomsten omtrent informatietransport aanwezig zijn.		
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
13.2.3	Elektronische berichten: Informatie die is opgenomen in elektronische berichten behoord passend te zijn beschermd.	n.v.t	n.v.t	Ontbreken control in SOC geaccepteerd door werkgroep. Geen informatie over beveiliging van elektronische berichten opgenomen in assurance rapportages. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Hieruit is op te maken dat Microsoft op gepaste wijze informatie beschermt die betrokken is bij elektronische berichten. Microsoft handhaaft de vertrouwelijkheid en integriteit van informatie tijdens de voorbereiding voor verzending en tijdens ontvangst. Per interview met Microsoft hebben wij vernomen dat Azure momenteel geen e-mailservers voor zijn klanten host. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien uit bovenstaande is op te maken dat informatie die is opgenomen in elektronische berichten wordt beschermd (indien van toepassing). Tevens heeft ook de klant hier een grote verantwoordelijkheid, zoals beschreven in de CUEC bij 13.2.3.1.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
13.2.3.1	Voor de beveiliging van elektronische (e-mail)berichten gelden de vastgestelde open standaarden tegen phishing en afluisteren op de 'pas toe of leg uit'-lijst van het Forum. Voor beveiliging van websiteverkeer gelden de open standaarden tegen afluisteren op de 'pas toe of leg uit'-lijst van het Forum.	n.v.t	n.v.t	Ontbreken control in SOC geaccepteerd door werkgroep. De standaarden zoals in de lijst van het Forum (SPF, DMARC en DKIM) zijn niet expliciet opgenomen in de Azure en M365 rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft beschermt op gepaste wijze informatie die betrokken is bij elektronische berichten. Microsoft handhaaft de vertrouwelijkheid en integriteit van informatie tijdens de voorbereiding voor verzending en tijdens ontvangst. Procedures voor de behandeling van bedrijfsmiddelen in verschillende vormen zijn in overeenstemming met de relevante normen en procedures. Azure: Per interview met Microsoft hebben wij vernomen dat Azure momenteel geen e-mailservers voor zijn klanten host. Uit bovenstaande is niet op te maken of gebruik wordt gemaakt van de standaarden zoals opgenomen in de lijst van het Forum. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien de gebruikersorganisatie verantwoordelijk is voor het inrichten van SPF, DMARC en DKIM voor M365.		Algemeen - CUEC: De gebruikersorganisaties is verantwoordelijk voor het inrichten van SPF, DMARC en DKIM voor M365.
13.2.3.2	Voor veilige berichtenuitwisseling met basisregistraties wordt, conform de 'pas toe of leg uit'-lijst van het Forum, gebruik gemaakt van de actuele versie van Digikoppeling.	n.v.t	n.v.t	Ontbreken control in SOC geaccepteerd door werkgroep. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is vanuit Microsoft en/of assurance rapportage aangezien geen sprake is van berichtenuitwisseling met basisregistraties.		
13.2.3.3	Maak gebruik van PKIoverheid-certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenen.	n.v.t	n.v.t	Ontbreken control in SOC geaccepteerd door werkgroep. Gebruik PKIoverheid certificaten niet opgenomen in Azure en M365 rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Hieruit is niet op te maken dat gebruik wordt gemaakt van PKIoverheid-certificaten. Per interview met Microsoft hebben wij vernomen dat voor de diensten van Microsoft intern eigen certificaten van de serviceorganisatie worden gebruikt, en dat het certificaat van Microsoft gelijk staat aan PKI-overheid certificaat. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien de gebruikersorganisatie verantwoordelijk is voor het gebruikmaken van PKI-overheidscertificaten.		Algemeen - CUEC: Gebruikers kunnen gebruik maken van PKI overheids-certificaten voor connecties van klant naar service. Dit is de verantwoordelijkheid van de gebruikersorganisatie.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
13.2.3.4	Om zekerheid te bieden over de integriteit van het elektronische bericht, wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard.	n.v.t	n.v.t	Ontbreken control in SOC geaccepteerd door werkgroep. Gebruik AdES Baseline Profile standaard niet opgenomen in Azure en M365 rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Hieruit is niet op te maken dat gebruik wordt gemaakt van de AdES Baseline Profile standaard voor elektronische handtekeningen. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is aangezien de gebruikersorganisatie verantwoordelijk is voor de inrichting van digitale handtekeningen.		Algemeen - CUEC: De gebruikersorganisaties is verantwoordelijk voor de inrichting van digitale handtekeningen ter bescherming van de integriteit van de documentformaten die vallen onder de AdES Baseline Profile standaard (XML-, CMS-, PDF- en ZIP-bestanden).

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst: Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	ELC-08	SOC2 - 13	Controls aanwezig in FedRAMP-raamwerk Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten en de beoordeling daarvan niet opgenomen in assurance rapportages. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor M365 op te maken dat de 'Microsoft Employee Handbook, confidentiality, non-disclosure, and M365 Rules of Behavior, and Master Supplier Services Agreement (MSSA)' jaarlijks worden herzien en bijgewerkt als gevolg van wijzigingen in wet- en regelgevende vereisten. Microsoft Corporate, External Legal Affairs (CELA) onderhoudt een sterk partnerschap met HR om ervoor te zorgen dat alle beleidsupdates wettelijk in overeenstemming zijn en geschikt zijn voor het bedrijf. Dit is opgenomen onder PS-6 in de M365 FedRAMP-rapportage.	Controls aanwezig in FedRAMP-raamwerk Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten en de beoordeling daarvan niet opgenomen in assurance rapportages. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor Azure op te maken dat Microsoft de Non-Disclosure Agreement (NDA), de Microsoft Security Policy en ander contractueel papierwerk dat wordt ondertekend door nieuwe werknemers ten minste jaarlijks beoordeelt. Als er wijzigingen nodig zijn, werkt Microsoft het papierwerk bij tijdens de jaarlijkse opnieuw bekijken. Het papierwerk wordt minimaal eens in de drie jaar bijgewerkt. Dit is opgenomen onder PL-04 in de Azure FedRAMP-rapportage.	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
14.1.1	Analyse en specificatie van informatiebeveiligingseisen: De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	CA-03	SDL - 1 SDL - 2	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	M365 - CUEC-06: De gebruikersorganisaties is verantwoordelijk voor het beveiligen van de software en hardware die worden gebruikt om toegang te krijgen tot M365. M365 - CUEC-08: De gebruikersorganisaties is verantwoordelijk voor het melden van geïdentificeerde beveiligings-, beschikbaarheids-, verwerkingsintegriteits - en vertrouwelijkheidsproblemen. M365 - CUEC-10/Azure: De gebruikersorganisaties is verantwoordelijk voor het begrijpen en naleven van de inhoud van hun servicecontracten, inclusief verplichtingen met betrekking tot systeembeveiliging, beschikbaarheid, verwerkingsintegriteit en vertrouwelijkheid.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
14.1.1.1	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de BIO.	n.v.t	n.v.t	Ontbreken control in SOC geaccepteerd door werkgroep. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is vanuit Microsoft en/of assurance rapportage aangezien deze verantwoordelijkheid bij de gebruikersorganisatie ligt.		Zie 14.1.1
14.1.2	Toepassingen op openbare netwerken beveiligen: Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	CA-44	DS - 2	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
14.1.3	Transacties van toepassingen beschermen: Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	n.v.t.	n.v.t	Ontbreken control in SOC geaccepteerd door werkgroep. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien de verantwoordelijkheid voor het beschermen van transacties van toepassingen niet ligt bij Microsoft maar bij de gebruikersorganisatie.		Algemeen - CUEC: De gebruikersorganisaties is verantwoordelijkheid voor het beschermen van transacties van toepassingen.
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
14.2.1	Beleid voor beveiligd ontwikkelen: Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.	CA-18 CA-21 CA-38 CA-46	CM - 1 CM - 6 SOC2 - 15 CM - 11	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het volgen van een Secure Development Lifecycle-methodologie voor haar applicaties die zijn ontwikkeld op Azure. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor de kwaliteits-borging van de applicatie voordat deze naar de Azure-productieomgeving wordt gebracht. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het bewaken van de beveiliging van haar applicaties die op Azure zijn ontwikkeld.
14.2.1.1	De gangbare principes rondom ‘security by design’ zijn uitgangspunt voor de ontwikkeling van software en systemen.	CA-21	CM - 1 CM - 6 SOC2 - 15 CM - 11	Controls aanwezig in ISO control mapping / NIST raamwerk Uit assurance rapportages van Azure en M365 niet op te maken dat alle gangbare principes rondom ‘security by design’ uitgangspunt zijn voor de ontwikkeling van software en systemen. Voor M365 is daarnaast niet op te maken dat het beleid omtrent wijzigingen expliciet is uiteengezet in controls. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Microsoft heeft regels voor de ontwikkeling van software en systemen opgesteld en toegepast		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				op ontwikkelingen binnen de organisatie. M365 beheert het informatiesysteem met behulp van een Security Development Lifecycle (SDL) waarin informatiebeveiligingsoverwegingen zijn opgenomen. Het proces Microsoft Security Development Lifecycle (https://www.microsoft.com/en-us/sdl/default.aspx) (SDL) wordt gevolgd voor engineering- en ontwikkelingsprojecten. Het SDL-proces omvat de volgende fasen waarin standaardprincipes voor beveiligingstechniek worden geïmplementeerd voor alle M365-systemen: - Fase 1: Vereiste. - Fase 2: Ontwerp. - Fase 3: Implementatie. - Fase 4: Verificatie. - Fase 5: Vrijgeven. Voorafgaand aan de release zijn definitieve beveiligings- en privacybeoordelingen vereist. Zoals vastgesteld door het M365-informatiebeveiligingsbeleid, moeten wijzigingen in de toepassingscode worden beoordeeld en goedgekeurd door het M365-beveiligingsteam. SDL Track is de online tool die wordt gebruikt om de voortgang van engineeringinitiatieven te volgen en het proces te controleren om ervoor te zorgen dat stappen worden gevolgd. De systeemeigenaar is verantwoordelijk om ervoor te zorgen dat het SDL-proces wordt gevolgd voor engineeringinitiatieven die verband houden met M365. Azure ontwikkelt plannen voor beveiligingsbeoordeling in overeenstemming met het Security Development Lifecycle-proces (SDL) van Microsoft. Alle ontwikkeling in Azure moet het Security Development Lifecycle-proces (SDL) volgen voor alle engineering- en ontwikkelingsprojecten. Het SDL-proces omvat het volgende: het aanpakken van beveiligingsvereisten; Identificeren van standaarden en tools/documenten tools en configuraties; Documenteert, beheert en waarborgt de integriteit van wijzigingen. Beveiligingstests vinden plaats tijdens de volgende fasen van het proces: Fase 3 – Implementatie, Fase 4 – Verificatie, Fase 5 – Vrijgave. Uit bovenstaande is op te maken dat security by design gehanteerd wordt als uitgangspunt bij het ontwikkelen van software en systemen.		
14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen: Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	CA-18 CA-21 CA-38 CA-46	CM - 1 CM - 6 SOC2 - 15 CM - 11	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
14.2.2.1	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework.	CA-18 CA-21 CA-38 CA-46	CM - 1 CM - 6 SOC2 - 15 CM - 11	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
14.2.3	Technische beoordeling van toepassingen na wijzigingen besturingsplatform: Als besturingsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	CA-21 CA-38 CA-46	CM - 2 CM - 4 CM - 5 CM - 10 CM - 13	Controls aanwezig in ISO control mapping / NIST raamwerk Geen controls opgenomen in assurance rapportage omtrent technische beoordeling van toepassingen na wijzigingen besturingsplatform. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. Microsoft beoordeelt en test bedrijfskritieke applicaties om er zeker van te zijn dat er geen nadelige gevolgen zijn voor de bedrijfsvoering of beveiliging wanneer besturingsplatforms worden gewijzigd. Microsoft test, valideert en documenteert wijzigingen in het M365-informatiesysteem voordat de wijzigingen in het besturingssysteem worden geïmplementeerd. Het M365-team volgt het Security Development Lifecycle (SDL)-proces, dat bestaat uit testen in een gescheiden omgeving, code-review en documentatie van wijzigingen binnen een tool voor wijzigingsbeheer. Technische beoordelingen van belangrijke M365-systeemwijzigingen worden uitgevoerd en goedgekeurd door wijzigingsadviesraden. Hieruit is op te maken dat bedrijfskritische toepassingen worden beoordeeld en getest als besturingsplatforms zijn veranderd.	Controls aanwezig in FedRAMP-raamwerk Geen controls opgenomen in assurance rapportage omtrent technische beoordeling van toepassingen na wijzigingen besturingsplatform. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is op te maken dat de risicobeoordeling wordt geüpdatet in geval van significante wijzigingen aan het systeem of de omgeving, waaronder een belangrijke wijziging in het besturingssysteem of de uitvoerende software. Dit is opgenomen onder RA-03 in de Azure FedRAMP-rapportage.	M365 - CUEC-06: De gebruikersorganisaties is verantwoordelijk voor het beveiligen van de software en hardware die worden gebruikt om toegang te krijgen tot M365.
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
14.2.4	(Vervallen)					
14.2.5	Principes voor engineering van beveiligde systemen: Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	CA-03 CA-11 CA-46	CM - 7 CM - 8 CM - 10	Controls aanwezig in ISO control mapping / NIST raamwerk Uit assurance rapportages van Azure en M365 niet op te maken dat alle gangbare principes rondom 'security by design' uitgangspunt zijn voor de ontwikkeling van software en systemen. Voor M365 is daarnaast niet op te maken dat het beleid omtrent wijzigingen expliciet is uiteengezet in controls. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Microsoft heeft regels voor de ontwikkeling van software en systemen opgesteld en toegepast op ontwikkelingen binnen de organisatie. M365 beheert het informatiesysteem met behulp van een Security Development Lifecycle (SDL) waarin informatiebeveiligingsoverwegingen zijn opgenomen. Het proces Microsoft Security Development Lifecycle (https://www.microsoft.com/en-us/sdl/default.aspx) (SDL) wordt gevolgd voor engineering- en ontwikkelingsprojecten. Het SDL-proces omvat de volgende fasen waarin standaardprincipes voor beveiligingstechniek worden geïmplementeerd voor alle M365-systemen: - Fase 1: Vereiste. - Fase 2: Ontwerp. - Fase 3: Implementatie. - Fase 4: Verificatie. - Fase 5: Vrijgeven. Voorafgaand aan de release zijn definitieve beveiligings- en privacybeoordelingen vereist. Zoals vastgesteld door het M365-informatiebeveiligingsbeleid, moeten wijzigingen in de toepassingscode worden beoordeeld en goedgekeurd door het M365-beveiligingsteam. SDL Track is de online tool die wordt gebruikt om de voortgang van engineeringinitiatieven te volgen en het proces te controleren om ervoor te zorgen dat stappen worden gevolgd. De systeemeigenaar is verantwoordelijk om ervoor te zorgen dat het SDL-proces wordt gevolgd voor engineeringinitiatieven die verband houden met M365. Azure ontwikkelt plannen voor beveiligingsbeoordeling in overeenstemming met het Security Development Lifecycle-proces (SDL) van Microsoft. Alle ontwikkeling in Azure moet het Security Development Lifecycle-proces (SDL) volgen voor alle engineering- en ontwikkelingsprojecten. Het SDL-proces omvat het volgende: het aanpakken van beveiligingsvereisten; Identificeren van standaarden en tools/documenten tools en configuraties; Documenteert, beheert en waarborgt de integriteit van wijzigingen. Beveiligingstests vinden plaats tijdens de volgende fasen van het proces: Fase 3 – Implementatie, Fase 4 – Verificatie, Fase 5 – Vrijgave. Uit bovenstaande is voldoende op te maken dat security by design gehanteerd wordt als uitgangspunt bij het ontwikkelen van software en systemen.		
14.2.5.1	Zie overheidsmaatregel 14.2.1.1			Zie overheidsmaatregel 14.2.1.1		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
14.2.6	Beveiligde ontwikkelomgeving: Organisaties behoren beveiligde ontwikkelomgevingen op te maken en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	n.v.t.	SDL - 4 *DEV-10*	Controls aanwezig in FedRAMP-raamwerk Controls hebben geen expliciete betrekking op de beveiliging van de ontwikkelomgeving. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft creëert en beschermt veilige ontwikkelomgevingen voor systeemontwikkeling en integratie-inspanningen die de gehele ontwikkelingslevenscyclus dekken. Microsoft integreert het risicobeheerproces voor informatiebeveiliging in de organisatie in Security Development Lifecycle (SDL)-activiteiten (zie ook 14.2.6.1). Azure: de eigenaar van het Azure-systeem is ervoor verantwoordelijk dat alle systeemontwikkelings- en onderhoudsactiviteiten worden uitgevoerd in overeenstemming met het Microsoft SDL-proces. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is tevens op te maken dat Microsoft het SDL-proces voortdurend beoordeelt om ervoor te zorgen dat het proces, standaarden en geselecteerde en gebruikte tools voldoende beveiliging bieden voor alle systemen en software ontwikkeld en uitgebracht door Microsoft. Dit is opgenomen onder SA-15 in de M365 en Azure FedRAMP-rapportage.		Azure CUEC: Gebruikersorganisatie is verantwoordelijk voor het gebruik van een beveiligde ontwikkelomgeving wanneer toepassingen worden ontwikkeld binnen het Azure platform.
14.2.6.1	Systeemontwikkelomgevingen worden passend beveiligd op basis van een expliciete risicoafweging.	n.v.t.	SDL - 4 *DEV-10*	Controls aanwezig in ISO control mapping / NIST raamwerk Controls hebben geen expliciete betrekking op de beveiliging van de ontwikkelomgeving. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft creëert en beschermt veilige ontwikkelomgevingen voor systeemontwikkeling en integratie-inspanningen die de gehele ontwikkelingslevenscyclus dekken. Microsoft integreert het risicobeheerproces voor informatiebeveiliging in de organisatie in Security Development Lifecycle (SDL)-activiteiten. De implementatie van levenscyclusondersteuning door M365 wordt beschreven in de Microsoft Security Development Lifecycle (https://www.microsoft.com/en-us/sdl/default.aspx). Dit proces wordt gevolgd door engineering- en ontwikkelingsprojecten. Voor systeemontwikkelingsprojecten moet een analyse van beveiligingsvereisten worden voltooid. Dit analysedocument fungeert als een raamwerk en omvat de identificatie van mogelijke risico's voor het voltooide ontwikkelingsproject, evenals mitigatiestrategieën die tijdens de ontwikkelingsfasen kunnen worden geïmplementeerd en getest. Tijdens de ontwikkelingslevenscyclus zijn kritische veiligheidscontroles en controlepunten voor goedkeuring opgenomen. Leden van softwareontwikkelingsteams krijgen passende training om op de hoogte te blijven van beveiligingspraktijken.		Azure CUEC: Gebruikersorganisatie is verantwoordelijk voor het gebruik van een beveiligde ontwikkelomgeving wanneer toepassingen worden ontwikkeld binnen het Azure platform.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				Azure: de eigenaar van het Azure-systeem is ervoor verantwoordelijk dat alle systeemontwikkelings- en onderhoudsactiviteiten worden uitgevoerd in overeenstemming met het Microsoft SDL-proces. Uit bovenstaande is voor Azure niet op te maken of de ontwikkelomgevingen passend worden beveiligd op basis van een expliciete risicoafweging.		
14.2.7	Uitbestede softwareontwikkeling: Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	n.v.t.	*DEV-02*	Niet van toepassing Microsoft maakt geen gebruik van uitbestede softwareontwikkeling, derhalve is deze control niet van toepassing.	Niet van toepassing Azure maakt geen gebruik maakt van uitbestede softwareontwikkeling, derhalve is deze control niet van toepassing.	
14.2.7.1	Een voorwaarde voor uitbestedingstrajecten is een expliciete risicoafweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd.	n.v.t.	*DEV-02*	Niet van toepassing Microsoft maakt geen gebruik van uitbestede softwareontwikkeling, derhalve is deze control niet van toepassing.	Niet van toepassing Azure maakt geen gebruik maakt van uitbestede softwareontwikkeling, derhalve is deze control niet van toepassing.	
14.2.8	Testen van systeembeveiliging: Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	CA-21 CA-38 CA-46	CM - 4 CM - 5 CM - 8 CM - 10	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
14.2.9	Systeemacceptatietests: Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	CA-18 CA-21 CA-38 CA-46	CM - 1 CM - 2 CM - 4 CM - 8 CM - 9 CM - 10	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
14.2.9.1	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	CA-18 CA-21 CA-38 CA-46	CM - 1 CM - 2 CM - 4 CM - 8 CM - 9 CM - 10	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
14.2.9.2	Van de resultaten van de testen wordt verslag gemaakt.	CA-18 CA-21 CA-38 CA-46	CM - 1 CM - 2 CM - 4 CM - 8 CM - 9 CM - 10	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
14.3.1	Bescherming van testgegevens: Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.	CA-21	SLD - 4 CM - 1 CM - 2 CM - 4 CM - 8 CM - 9 CM - 10	Controls aanwezig in ISO control mapping/NIST raamwerk In de M365 assurance rapportage is de bescherming van testgegevens niet expliciet opgenomen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. Microsoft selecteert, beschermt en controleert testgegevens zorgvuldig. Microsoft vereist dat de ontwikkelaar van een M365-informatiesysteem, systeemonderdeel of informatiesysteemservice een beveiligingsbeoordelingsplan maakt en implementeert. In overeenstemming met de Microsoft Security Development Lifecycle (SDL) vinden beveiligingstests plaats in verschillende fasen tijdens het SDL-proces. Beveiligingstests vinden met name plaats tijdens de volgende fasen van de SDL: implementatie, verificatie en release. Uit bovenstaande is op te maken dat	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				maatregelen zijn getroffen omtrent de bescherming van testgegevens.		
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties: Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.	ELC-12 ELC-15 CA-53	ELC - 6 SOC2 - 25	Controls aanwezig in FedRAMP-raamwerk Uit assurance rapportages van Azure en M365 niet expliciet op te maken of informatiebeveiligingseisen worden overeengekomen met de leveranciers. Uit aanvullende ontvangen FedRAMP-rapportages (geen assurance) is op te maken dat Azure acquisitiecontrole implementeert door handhaving van de Microsoft Security Policy. Het Beleid schrijft voor dat [...] in een formeel contract afspraken moeten worden gemaakt om de verantwoordelijkheid en vereisten voor de beveiliging, vertrouwelijkheid, integriteit en beschikbaarheid van de betrokken informatiemiddelen te definiëren. Passende beveiligingsnormen worden in de overeenkomst opgenomen, om voor geïdentificeerde risico's een beschermingsniveau te hebben gelijkwaardig aan het Microsoft-beveiligingsbeleid. Het is de rol van Corporate, External and Legal Affairs (CELA) om tekst op te nemen in systeemacquisitiecontracten met betrekking tot de beveiligingsvereisten, door middel van de		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				Master Supplier Services Agreement (MSSA) of een equivalent daarvan. Dit is opgenomen onder SA-04 in de Azure FedRAMP-rapportage. Tevens is uit ontvangen FedRAMP-rapportages (geen assurance) op te maken dat Microsoft alleen derden inschakelt die een Microsoft Master Vendor Agreement (MMVA) hebben ondertekend en zijn goedgekeurd door het inkoop- en CELA-team. De MMVA vereist dat de derde partij voldoet aan alle toepasselijke beveiligingsbeleidsregels van Microsoft, beveiligingsprocedures implementeert om openbaarmaking van vertrouwelijke informatie van Microsoft te voorkomen, hun eigen informatiebeveiligingsprogramma implementeert en vereist dat de leverancier alle relevante informatie verstrekt die de functionele eigenschappen van de beveiligingscontroles beschrijft werkzaam binnen het systeem. Dit is opgenomen onder SA-4 in de M365 FedRAMP-rapportage.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
15.1.1.1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden eisen ten aanzien van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd. Deze eisen zijn gebaseerd op een expliciete risicoafweging.	ELC-12 ELC-15 CA-53	ELC - 6 SOC2 - 25	Controls aanwezig in FedRAMP-raamwerk Uit assurance rapportages van Azure en M365 niet op te maken dat eisen ten aanzien van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) worden benoemd in offerteaanvragen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365. M365: Microsoft gaat overeenkomsten aan met leveranciers en documenteert informatiebeveiligingsvereisten om de risico's te verminderen die gepaard gaan met de toegang van leveranciers tot de bedrijfsmiddelen van de organisatie. Externe providers moeten een geheimhoudingsverklaring ondertekenen voordat ze toegang krijgen tot M365-informatiesystemen of bedrijfsinformatie. Microsoft stemt in met en handhaaft informatiebeveiligingsvereisten voor M365-leveranciers via de Interconnection Security Agreements (ISA's). Uit bovenstaande is op te maken dat voor M365 de informatiebeveiligingsvereisten worden vastgelegd via de ISA's. Voor M365 is niet expliciet op te maken dat eisen omtrent vertrouwelijkheid, integriteit en beschikbaarheid gesteld zijn. Uit aanvullende ontvangen FedRAMP-rapportage van M365 (geen assurance) is op te maken dat Microsoft vereist dat alle derde partijen (externe informatiesysteemservices) die betrokken zijn bij M365 een Master Supplier Services Agreement (MSSA) ondertekenen. De MSSA vereist dat de derde partij voldoet aan alle toepasselijke beveiligingsbeleidsregels van	Controls aanwezig in ISO control mapping / NIST raamwerk Uit assurance rapportages van Azure en M365 niet op te maken dat eisen ten aanzien van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) worden benoemd in offerteaanvragen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over het NIST-framework (2021) voor Azure. Azure: Microsoft documenteert beveiligingsvereisten van derden in het Microsoft Information Security Policy en bijbehorende standaarden. Subverwerkers zijn verplicht om de vertrouwelijkheid van deze gegevens te bewaren en zijn contractueel verplicht om te voldoen aan strikte privacyvereisten die gelijkwaardig zijn aan of sterker zijn dan de contractuele toezeggingen die Microsoft aan haar klanten doet in de Voorwaarden voor Online Services. Subverwerkers zijn ook verplicht om te voldoen aan de vereisten van de Algemene Verordening Gegevensbescherming (AVG) van de EU, inclusief die met betrekking tot het implementeren van passende technische en organisatorische maatregelen om persoonsgegevens te beschermen. Microsoft vereist dat subverwerkers deelnemen aan het Microsoft Supplier Security and Privacy Assurance Program. Dit programma is ontworpen om de gegevensverwerkingspraktijken te standaardiseren en te versterken en om ervoor te zorgen dat de bedrijfsprocessen en -systemen van leveranciers consistent	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				Microsoft en beveiligingsprocedures implementeert om openbaarmaking van vertrouwelijke informatie van Microsoft te voorkomen. Microsoft neemt bepalingen op in de MSSA en alle bijbehorende Statements of Work (SOW) van iedere leverancier die ingaan op de noodzaak om passende beveiligingsmaatregelen te nemen. Leveranciers die gevoelige gegevens verwerken, moeten voldoen aan de privacypraktijken en gegevensbeschermingsvereisten van Microsoft-leveranciers.	zijn met die van Microsoft. Voor subverwerkers die toegang hebben tot klantgegevens en persoonsgegevens gelden hogere eisen. Microsoft schakelt alleen die derden in die een contract hebben ondertekend en zijn goedgekeurd door de teams Procurement en Microsoft Corporate, External and Legal Affairs (CELA). In overeenstemming met de MSSA vereisen contracten dat de derde partij beveiligingsprocedures implementeert om openbaarmaking van vertrouwelijke informatie van Microsoft te voorkomen en alle relevante informatie te verstrekken die de functionele vereisten of specificaties beschrijft van de beveiligingscontroles die binnen het systeem moeten worden toegepast. Bovendien moeten derden die toegang hebben tot de Azure-omgeving een formeel contract hanteren waarin de verantwoordelijkheden en vereisten zijn vastgelegd voor het handhaven van de beveiliging, vertrouwelijkheid, integriteit en beschikbaarheid van de informatie-assets die bij het contract zijn betrokken. Uit bovenstaande is voor Azure op te maken dat specifiek aandacht is voor de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie-assets die bij het contract zijn betrokken.	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
15.1.1.2	Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekking tot leverancierstoegang tot bedrijfsinformatie vastgesteld.	ELC-12 ELC-15 CA-53	ELC - 6 SOC2 - 25	Controls aanwezig in ISO control mapping / NIST raamwerk Uit assurance rapportages van Azure en M365 niet op te maken dat de risicoafweging betrekking heeft op toegang tot bedrijfsinformatie. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365. M365: Microsoft gaat overeenkomsten aan met leveranciers en documenteert informatiebeveiligingsvereisten om de risico's te verminderen die gepaard gaan met de toegang van leveranciers tot de bedrijfsmiddelen van de organisatie. Microsoft stelt beveiligingsvereisten voor personeel vast, waaronder beveiligingsrollen en -verantwoordelijkheden voor externe providers. Beleid en richtlijnen voor uitzendkrachten en leveranciers zijn te vinden op interne bedrijfswebsites. In contracten neemt Microsoft bepalingen op om ervoor te zorgen dat externe leveranciers voldoen aan de door Microsoft opgelegde personeelsbeveiligingsvereisten of deze overtreffen. Dit omvat de mogelijkheid om met succes de Microsoft Cloud Background Check of het equivalent daarvan te doorstaan, evenals het verkrijgen en behouden van een goedkeuring als het specifieke project dit vereist. Externe providers zijn onderworpen aan dezelfde vereisten voor personeelsscreening als Microsoft-medewerkers die werken aan het M365-systeem voor federale klanten. Externe providers moeten een geheimhoudingsverklaring ondertekenen voordat ze toegang krijgen tot M365-informatiesystemen of bewonersinformatie. Microsoft stemt in met en handhaaft informatiebeveiligingsvereisten voor M365-	Controls aanwezig in FedRAMP-raamwerk Uit assurance rapportages van Azure en M365 niet op te maken dat de risicoafweging betrekking heeft op toegang tot bedrijfsinformatie. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over het NIST-framework (2021) voor Azure. Voor Azure is niet op te maken dat de eisen/maatregelen omtrent leverancierstoegang vastgesteld worden op basis van een expliciete risicoafweging Uit aanvullende ontvangen FedRAMP-rapportages (geen assurance) is op te maken dat Azure acquisitiecontrole implementeert door handhaving van de Microsoft Security Policy. Passende beveiligingsnormen worden in de overeenkomst opgenomen, om voor geïdentificeerde risico's een beschermingsniveau te hebben gelijkwaardig aan het Microsoft-beveiligingsbeleid. Dit is opgenomen onder SA-04 in de Azure FedRAMP-rapportage.	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				leveranciers via de Interconnection Security Agreements (ISA's). Uit bovenstaande is op te maken dat voor M365 expliciet overeenkomsten worden aangegaan omtrent beveiligingseisen om het risico van leverancierstoegang te mitigeren.		
15.1.1.3	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.	ELC-12 ELC-15 CA-53	ELC - 6 SOC2 - 25	Controls aanwezig in ISO control mapping / NIST raamwerk Niet specifiek vermeld in de assurance rapportages. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft vereist dat leveranciers van externe informatiesysteemservices voldoen aan de informatiebeveiligingsvereisten van de organisatie en beveiligingscontroles in overeenstemming met de toepasselijke federale wetten, uitvoeringsbesluiten, richtlijnen, beleidslijnen, voorschriften, normen en richtlijnen. Microsoft vereist dat derden (externe informatiesysteemservices) die met Microsoft zijn verbonden een Microsoft Master Vendor Agreement (MMVA) en Interconnection Security Agreements (ISA's) ondertekenen. De MMVA en ISA's vereisen dat de derde partij voldoet aan het toepasselijke M365-beveiligingsbeleid en beveiligingsprocedures implementeert om openbaarmaking van vertrouwelijke informatie van Microsoft te voorkomen. Microsoft neemt bepalingen op in de MMVA en alle bijbehorende Statement of Work (SOW) waarbij elke leverancier ingaat op de noodzaak om passende beveiligingsmaatregelen te nemen. Leveranciers die gevoelige gegevens verwerken, moeten voldoen aan de privacypraktijken en gegevensbeschermings-vereisten van M365-leveranciers. Azure: Azure deelt persoonlijk identificeerbare informatie (PII) met externe derden, ook wel subverwerkers genoemd op grond van speciale overeenkomsten die de overdracht van PII toestaan. Privacy-SOP's worden gebruikt in combinatie met het extern delen van PII. Subverwerkers zijn verplicht om de vertrouwelijkheid van deze gegevens te bewaren en zijn contractueel verplicht om te voldoen aan strikte privacyvereisten die gelijkwaardig zijn aan of sterker zijn dan de contractuele toezeggingen die Microsoft aan haar klanten doet in de Voorwaarden voor Online Services. Subverwerkers zijn ook verplicht om te voldoen aan de vereisten van de Algemene Verordening Gegevensbescherming (AVG) van de EU, inclusief die met betrekking tot het implementeren van passende technische en organisatorische maatregelen om persoonsgegevens te beschermen. Microsoft vereist dat subverwerkers deelnemen aan het Microsoft Supplier Security and Privacy Assurance Program. Dit programma is ontworpen om de gegevensverwerkingspraktijken te standaardiseren en te versterken en om ervoor te zorgen dat de bedrijfsprocessen en -systemen van leveranciers		Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor de naleving van toepasselijke wet-/regelgeving.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				consistent zijn met die van Microsoft. Voor subverwerkers die toegang hebben tot klantgegevens en persoonsgegevens gelden hogere eisen. Uit bovenstaande is op te maken dat voor Azure en M365 eisen worden gesteld aan het voldoen aan (bijvoorbeeld) de AVG en 'toepasselijke federale wetten' door de subverwerkers/leveranciers, echter is hieruit niet op te maken of deze (en andere wettelijk vereiste afspraken) in een verwerkersovereenkomst worden vastgelegd.		
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	ELC-12 ELC-15 CA-53	ELC - 6 SOC2 - 25	Controls aanwezig in FedRAMP-raamwerk Uit assurance rapportages van Azure en M365 niet expliciet op te maken of informatiebeveiligingseisen worden overeengekomen met de leveranciers. Uit aanvullende ontvangen FedRAMP-rapportages (geen assurance) is op te maken dat Azure acquisitiecontrole implementeert door handhaving van de Microsoft Security Policy. Het Beleid schrijft voor dat [...] in een formeel contract afspraken moeten worden gemaakt om de verantwoordelijkheid en vereisten voor de beveiliging, vertrouwelijkheid, integriteit en beschikbaarheid van de betrokken informatiemiddelen te definiëren. Passende beveiligingsnormen worden in de overeenkomst opgenomen, om voor geïdentificeerde risico's een beschermingsniveau te hebben gelijkwaardig aan het Microsoft-beveiligingsbeleid. Het is de rol van Corporate, External and Legal Affairs (CELA) om tekst op te nemen in systeemacquisitiecontracten met betrekking tot de beveiligingsvereisten, door middel van de Master Supplier Services Agreement (MSSA) of een equivalent daarvan. Dit is opgenomen onder SA-04 in de Azure FedRAMP-rapportage. Tevens is uit ontvangen FedRAMP-rapportages (geen assurance) op te maken dat Microsoft alleen derden inschakelt die een Microsoft Master Vendor Agreement (MMVA) hebben ondertekend en zijn goedgekeurd door het inkoop- en CELA-team. De MMVA vereist dat de derde partij voldoet aan alle toepasselijke beveiligingsbeleidsregels van Microsoft, beveiligingsprocedures implementeert om openbaarmaking van vertrouwelijke informatie van Microsoft te voorkomen, hun eigen informatiebeveiligingsprogramma implementeert en vereist dat de leverancier alle relevante informatie verstrekt die de functionele eigenschappen van de beveiligingscontroles beschrijft werkzaam binnen het systeem. Dit is opgenomen onder SA-4 in de M365 FedRAMP-rapportage.		
15.1.2.1	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.	ELC-12 ELC-15 CA-53	ELC - 6 SOC2 - 25	Controls aanwezig in ISO control mapping / NIST raamwerk Uit assurance rapportages van Azure en M365 niet op te maken of beveiligingseisen uit de offerteaanvraag expliciet worden opgenomen in inkoopcontracten. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft stelt relevante informatiebeveiligingsvereisten vast en stemt ermee in met elke leverancier die IT-infrastructuurcomponenten voor M365 mag openen, verwerken,		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				opslaan, communiceren of leveren. Microsoft vereist dat leveranciers van externe informatiesysteemservices voldoen aan de informatiebeveiligingsvereisten van de organisatie en beveiligingscontroles in overeenstemming met de toepasselijke federale wetten, uitvoeringsbesluiten, richtlijnen, beleidslijnen, voorschriften, normen en richtlijnen. Microsoft vereist dat derden (externe informatiesysteemservices) die met Microsoft zijn verbonden een Microsoft Master Vendor Agreement (MMVA) en Interconnection Security Agreements (ISA's) ondertekenen. De MMVA en ISA's vereisen dat de derde partij voldoet aan het toepasselijke M365-beveiligingsbeleid en beveiligingsprocedures implementeert om openbaarmaking van vertrouwelijke informatie van Microsoft te voorkomen. Microsoft neemt bepalingen op in de MMVA en alle bijbehorende Statement of Work (SOW) waarbij elke leverancier ingaat op de noodzaak om passende beveiligingsmaatregelen te nemen. Leveranciers die gevoelige gegevens verwerken, moeten voldoen aan de privacypraktijken en gegevensbeschermingsvereisten van M365-leveranciers. Azure: Azure implementeert het acquisitiebeheer door het afdwingen van het Microsoft-beveiligingsbeleid. Het Beleid schrijft voor dat waar een derde partij toestemming heeft om (i) toegang te krijgen tot, de informatiemiddelen of informatieverwerkingsfaciliteiten van Microsoft's online diensten te openen, te verwerken, te hosten of te beheren, of (ii) producten of diensten toe te voegen aan de informatieverwerkingsfaciliteiten van de online diensten van Microsoft, regelingen moet worden vastgelegd in een formeel contract om de verantwoordelijkheid en vereisten voor de beveiliging, vertrouwelijkheid, integriteit en beschikbaarheid van de betrokken informatiemiddelen te definiëren. Passende beveiligingsstandaarden worden behandeld in de overeenkomst, om een niveau van bescherming te bieden tegen geïdentificeerde risico's dat gelijkwaardig is aan het beveiligingsbeleid van Microsoft. Het is de rol van Corporate, External and Legal Affairs (CELA) om taal te eisen die is opgenomen in systeemverwervingscontracten met betrekking tot de beveiligingsvereisten, indien van toepassing, via de Master Supplier Services Agreement (MSSA) of een gelijkwaardig type overeenkomst. Microsoft neemt voor elke leverancier bepalingen op in de MSA en alle bijbehorende Statements of Work (SOW) die ingaan op de noodzaak om passende beveiligingsmaatregelen te nemen. Uit bovenstaande is op te maken dat een vereiste is dat de M365/Microsoft beveiligingsbeleid en -procedures gehanteerd worden. Tevens wordt in de MSA/MMVA en SoW de noodzaak voor passende beveiligingsmaatregelen opgenomen. Hieruit is echter niet op te maken dat de beveiligingseisen uit de offerteaanvraag expliciet worden opgenomen in de (inkoop)contracten.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
15.1.2.2	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.	ELC-12 ELC-15 CA-53	ELC - 6 SOC2 - 25	Geen controls beschreven Uit assurance rapportages van Azure en M365 niet op te maken of prestatie-indicatoren en verantwoordingsrapportages worden opgenomen in inkoopcontracten. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Uit bovenstaande is niet op te maken of in de inkoopcontracten expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages worden opgenomen.		
15.1.2.3	In situaties waarin contractvoorwaarden worden opgelegd door leveranciers, is voorafgaand aan het tekenen van het contract met een risicoafweging helder gemaakt wat de consequenties hiervan zijn voor de organisatie. Expliciet is gemaakt welke consequenties geaccepteerd worden en welke gemitigeerd moeten zijn bij het aangaan van de overeenkomst.	ELC-12 ELC-15 CA-53	ELC - 6 SOC2 - 25	Controls aanwezig in ISO control mapping / NIST raamwerk Uit assurance rapportages van Azure en M365 niet op te maken dat alle aspecten opgenomen zijn in contractvoorwaarden. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft stelt relevante informatiebeveiligingsvereisten vast en stemt ermee in met elke leverancier die IT-infrastructuurcomponenten voor M365 mag openen, verwerken, opslaan, communiceren of leveren. Microsoft vereist dat leveranciers van externe informatiesysteemservices voldoen aan de informatiebeveiligingsvereisten van de organisatie en beveiligingscontroles in overeenstemming met de toepasselijke federale wetten, uitvoeringsbesluiten, richtlijnen, beleidslijnen, voorschriften, normen en richtlijnen. Microsoft vereist dat derden (externe informatiesysteemservices) die met Microsoft zijn verbonden een Microsoft Master Vendor Agreement (MMVA) en Interconnection Security Agreements (ISA's) ondertekenen. De MMVA en ISA's vereisen dat de derde partij voldoet aan het toepasselijke M365-beveiligingsbeleid en beveiligingsprocedures implementeert om openbaarmaking van vertrouwelijke informatie van Microsoft te voorkomen. Microsoft neemt voor elke leverancier bepalingen op in de MMVA en alle bijbehorende Statement of Work (SOW) die ingaan op de noodzaak om passende beveiligingsmaatregelen te nemen. Leveranciers die gevoelige gegevens verwerken, moeten voldoen aan de privacypraktijken en gegevensbeschermingsvereisten van M365-leveranciers. Azure: Microsoft schakelt leveranciersbureaus in via de externe tool van Microsoft, die is ontworpen voor derden (leveranciersbureaus) die een Master Service Agreement (MSA) hebben ondertekend en/of zijn goedgekeurd door de Global Procurement Group (GPG) als een "Approved Vendor" in specifieke werkcategorieën. GPG vereist dat de derde partij voldoet aan alle toepasselijke beveiligingsbeleidsregels van Microsoft en beveiligingsprocedures implementeert om openbaarmaking van vertrouwelijke informatie van Microsoft te voorkomen. Microsoft neemt voor elke leverancier bepalingen op in de MSA en alle bijbehorende Statements of Work (SOW) die ingaan op de noodzaak om passende beveiligingsmaatregelen te nemen. Bovendien moeten leveranciers die gegevens met een hoge zakelijke impact verwerken, jaarlijks voldoen aan het Microsoft Vendor Privacy		Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het begrijpen en naleven van de inhoud van hun servicecontracten, inclusief verplichtingen met betrekking tot systeembeveiliging, beschikbaarheid, verwerkingsintegriteit en vertrouwelijkheid.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				Assurance (VPA)-programma. Uit bovenstaande is op te maken dat een vereiste is dat de M365/Microsoft beveiligingsbeleid en -procedures gehanteerd worden. Tevens wordt in de MSA/MMVA en SoW de noodzaak voor passende beveiligingsmaatregelen opgenomen. Hieruit is echter niet op te maken dat expliciet wordt gemaakt welke consequenties geaccepteerd worden en welke gemitigeerd moeten zijn bij het aangaan van de overeenkomst.		
15.1.2.4	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaardvoorwaarden voor inkoop gehanteerd.	ELC-12 ELC-15 CA-53	ELC - 6 SOC2 - 25	Controls aanwezig in ISO control mapping / NIST raamwerk Uit assurance rapportages van Azure en M365 niet op te maken of standaardvoorwaarden voor inkoop worden gehanteerd. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft vereist dat derden (externe informatiesysteemservices) die met Microsoft zijn verbonden een Microsoft Master Vendor Agreement (MMVA) en Interconnection Security Agreements (ISA's) ondertekenen. De MMVA en ISA's vereisen dat de derde partij voldoet aan het toepasselijke M365-beveiligingsbeleid en beveiligingsprocedures implementeert om openbaarmaking van vertrouwelijke informatie van Microsoft te voorkomen. Microsoft neemt bepalingen op in de MMVA en alle bijbehorende Statement of Work (SOW) waarbij elke leverancier ingaat op de noodzaak om passende beveiligingsmaatregelen te nemen. Leveranciers die gevoelige gegevens verwerken, moeten voldoen aan de privacypraktijken en gegevensbeschermingsvereisten van M365-leveranciers. Azure: Microsoft schakelt leveranciersbureaus in via de externe besteltool van Microsoft, die is ontworpen voor derden (leveranciersbureaus) die een Master Service Agreement (MSA) hebben ondertekend en/of zijn goedgekeurd door de Global Procurement Group (GPG) als een “Approved Vendor” in specifieke werkcategorieën. GPG vereist dat de derde partij voldoet aan alle toepasselijke beveiligingsbeleidsregels van Microsoft en beveiligingsprocedures implementeert om openbaarmaking van vertrouwelijke informatie van Microsoft te voorkomen. Microsoft neemt bepalingen op in de MSA en alle bijbehorende Statements of Work (SOW) waarbij elke leverancier inspeelt op de noodzaak om passende beveiligingsmaatregelen te nemen. Bovendien moeten leveranciers die gegevens met een hoge zakelijke impact verwerken, jaarlijks voldoen aan het Microsoft Vendor Privacy Assurance (VPA)-programma. Uit bovenstaande is op te maken dat standaardvoorwaarden voor inkoop worden gehanteerd ter waarborging van vertrouwelijkheid of geheimhouding.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
15.1.2.5	Voordat een contract wordt afgesloten, wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exit-strategie.	ELC-12 ELC-15 CA-53	ELC - 6 SOC2 - 25	Geen controls beschreven Uit assurance rapportages van Azure en M365 niet op te maken dat de risicoafweging betrekking heeft op de afhankelijkheid. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Uit bovenstaande is voor M365 en Azure niet op te maken dat een expliciete uitwerking van de exit-strategie een vast onderdeel van het contract is.		
15.1.2.6	In inkoopcontracten wordt expliciet de mogelijkheid van een externe audit opgenomen waarmee de betrouwbaarheid van de geleverde dienst kan worden getoetst. Een audit is niet nodig als de contractant door middel van certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.	ELC-12 ELC-15 CA-53	ELC - 6 SOC2 - 25	Controls aanwezig in ISO control mapping / NIST raamwerk Uit assurance rapportages van Azure en M365 niet op te maken of afspraken over externe audits wordt opgenomen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft controleert, beoordeelt en audits de levering van leveranciersdiensten regelmatig. Microsoft gebruikt processen, methoden en technieken om de naleving van beveiligingscontroles door externe serviceproviders doorlopend te controleren. Microsoft ondertekent Interconnection Security Agreements (ISA's) met externe leveranciers van informatiesystemen indien nodig; ISA's definiëren M365-toezicht. Microsoft neemt bepalingen op in de Microsoft Master Vendor Agreement (MMVA) en alle bijbehorende Statement of Work (SOW) waarbij elke leverancier ingaat op de noodzaak om passende beveiligingsmaatregelen te gebruiken. Leveranciers die gevoelige gegevens verwerken, moeten voldoen aan de privacypraktijken en gegevensbeschermingsvereisten van Microsoft voor leveranciers. Azure: Azure autoriseert verbindingen van het informatiesysteem naar andere informatiesystemen buiten de autorisatiegrens door het gebruik van leveranciersovereenkomsten, Memoranda of Understanding (MOU's), Interconnection Security Agreements (ISA's), algemene voorwaarden (T&C) en/of service Level Agreements (SLA's). Microsoft heeft de nodige leveranciersovereenkomsten, MOU's, ISA's, T&C en SLA's ontwikkeld die verbindingen buiten de federale autorisatiegrens documenteren. Azure volgt de richtlijnen met betrekking tot overheidsinstanties in die zin dat Interconnection Security Agreements (ISA's) niet zijn ontworpen voor gebruik tussen een CSP en een Federaal Agentschap. Een ATO-memo van het Agentschap moet het leidende document zijn voor communicatie tussen het Agentschap en Azure en de communicatie over beveiligingsvereisten. De enige onderlinge verbindingen zijn tussen interne Microsoft-services, waarvoor geen ISA's nodig zijn. Op dit moment is Azure niet afhankelijk van informatiesystemen buiten Microsoft die ISA's vereisen. Uit bovenstaande is op te maken dat voor M365 regelmatig audits uitgevoerd worden bij leveranciers en dat ISA's getekend worden met leveranciers waarin het overzicht houden voor		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				M365 gedefinieerd wordt. Uit bovenstaande is tevens op te maken dat voor Azure ook ISA's getekend worden, echter is voor beide niet op te maken dat de mogelijkheid van een externe audit expliciet wordt opgenomen in inkoopcontracten. Wel is op te maken dat leveranciers die gegevens met een hoge zakelijke impact verwerken, jaarlijks moeten voldoen aan het Microsoft Vendor Privacy Assurance (VPA)-programma.		
15.1.3	Toeleveringsketen van informatie- en communicatietechnologie: Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	ELC-12 ELC-15 CA-53	ELC - 6 SOC2 - 25	Controls aanwezig in FedRAMP-raamwerk Uit assurance rapportages van Azure en M365 niet op te maken of overeenkomsten met leveranciers eisen bevatten omtrent de toeleveringsketen. Uit aanvullende ontvangen FedRAMP-rapportages (geen assurance) is voor Azure op te maken dat passende beveiligingsnormen in de overeenkomst worden opgenomen, om voor geïdentificeerde risico's een beschermingsniveau te hebben gelijkwaardig aan het Microsoft-beveiligingsbeleid. Het is de rol van Corporate, External and Legal Affairs (CELA) om tekst op te nemen in systeemacquisitiecontracten met betrekking tot de beveiligingsvereisten, door middel van de Master Supplier Services Agreement (MSSA) of een equivalent daarvan. Dit is opgenomen onder SA-04 in de Azure FedRAMP-rapportage. Tevens is uit ontvangen FedRAMP-rapportages (geen assurance) op te maken dat Microsoft alleen derden inschakelt die een Microsoft Master Vendor Agreement (MMVA) hebben ondertekend en zijn goedgekeurd door het inkoop- en CELA-team. Dit is opgenomen onder SA-4 in de M365 FedRAMP-rapportage. Per interview met Microsoft hebben wij vernomen dat eisen omtrent de toeleveringsketen zijn opgenomen in deze supplier/vendor agreements.		
15.1.3.1	Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.	ELC-12 ELC-15 CA-53	ELC - 6 SOC2 - 25	Geen controls beschreven Uit assurance rapportages van Azure en M365 niet op te maken of leveranciers hun toeleveranciers bekend moeten maken en eisen hieraan op leggen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Uit bovenstaande is niet op te maken dat leveranciers hun keten van toeleveranciers bekend moeten maken en transparant moeten zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers: Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	CA-53	ELC - 6 SOC2 - 25 BC - 6	Controls aanwezig in FedRAMP-raamwerk In assurance rapportage van M365 wordt enkel gesproken over monitoring van de afhankelijkheden van Azure door het opvragen van attestrapporten. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor M365 op te maken dat het de rol van Corporate, External and Legal Affairs (CELA) is om tekst op te nemen in systeemacquisitiecontracten met betrekking tot de beveiligingsvereisten. Dit bevat onder andere functionele beveiligingsvereisten, [...] en de vereisten voor assurance omtrent beveiliging. Dit is opgenomen onder SA-4 in de M365 FedRAMP-rapportage.	Controls aanwezig in FedRAMP-raamwerk In assurance rapportage van Azure wordt enkel gesproken over monitoring van contracten op inconsistenties en non-conformiteit. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor Azure op te maken dat leveranciers die gevoelige/bedrijfskritische data behandelen jaarlijks in overeenstemming moeten zijn met het Microsoft Vendor Privacy Assurance (VPA) programma. Dit is opgenomen onder SA-01 in de Azure FedRAMP-rapportage.	
15.2.1.1	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.	CA-53	ELC - 6 SOC2 - 25 BC - 6	Geen controls beschreven Uit assurance rapportages van Azure en M365 niet op te maken of de prestatie jaarlijks wordt beoordeeld op dezelfde indicatoren als opgenomen in contracten. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Uit bovenstaande is niet op te maken dat de prestatie van leveranciers op het gebied van informatiebeveiliging jaarlijks wordt beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.		
15.2.2	Beheer van veranderingen in dienstverlening van leveranciers: Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden beheerd, rekening houdend met de kritikaliteit van	n.v.t.	n.v.t.	Controls aanwezig in ISO control mapping / NIST raamwerk Uit assurance rapportage niet op te maken hoe veranderingen in de dienstverlening van leveranciers worden beheerd. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365.	Controls aanwezig in FedRAMP-raamwerk Uit assurance rapportage niet op te maken hoe veranderingen in de dienstverlening van leveranciers worden beheerd. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor Azure op te maken dat Azure de Interconnection Security Agreements (ISA's) bewaakt om de beveiligingsvereisten te verifiëren.	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
	bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.			Microsoft beheert wijzigingen in de dienstverlening door leveranciers, inclusief het onderhouden en verbeteren van bestaande informatiebeveiligingsbeleidslijnen, -procedures en -controles, rekening houdend met het kritieke karakter van de betrokken bedrijfsinformatie, systemen en processen en herbeoordeling van risico's. Microsoft voert een organisatorische risicobeoordeling uit voordat specifieke informatiebeveiligingsservices worden aangeschaft of uitbesteed. Als onderdeel van acquisitieactiviteiten wordt een risicobeoordeling van externe dienstverleners uitgevoerd. Externe leveranciers moeten de Microsoft Master Vendor Agreement (MMVA) ondertekenen, die een basisrisicobeoordeling van de leverancier als bedrijf omvat. Voor elke partij met wie Microsoft een Interconnection Security Agreement (ISA) tekent, komt Microsoft regelmatig met hen samen en controleert de overeenkomst en eventuele wijzigingen binnen de overeenkomst. Uit bovenstaande is op te maken dat processen omtrent beheer van veranderingen in dienstverlening van leveranciers aanwezig zijn.	Azure heeft jaarlijkse bijeenkomsten met derden om de overeenkomsten en eventuele wijzigingen te beoordelen. Azure zorgt ervoor dat de verbindingsgegevens die in ISA's worden beschreven, worden vastgelegd en bewaakt als onderdeel van het continue monitoringsproces van Azure. Dit is opgenomen onder CA-03 in de Azure FedRAMP-rapportage.	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
16.1.1	Verantwoordelijkheden en procedures: Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	CA-13 CA-17 CA-26 CA-29 CA-47	IM - 1 IM - 3 IS - 3	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in FedRAMP-raamwerk Uit assurance rapportage is een expliciete beschrijving van de directieverantwoordelijkheden omtrent informatiebeveiligingsincidenten niet herleidbaar. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor Azure op te maken dat twee typen informatiebeveiligingsbeleid zijn vastgesteld, waarin onder andere de rollen en verantwoordelijkheden zijn opgenomen, evenals procedures en training, en verplichtingen van het management. Dit is opgenomen onder IRs-01 in de Azure FedRAMP-rapportage.	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	CA-13 CA-16 CA-17 CA-26 CA-29 CA-47	IM - 1 IM - 2 IM - 3 IM - 4 IM - 5 IM - 6	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure en M365 - CUEC: De gebruikersorganisatie is verantwoordelijk voor het aan Microsoft rapporteren van de incidenten en waarschuwingen die specifiek zijn voor hun systemen en Azure. Voor dit rapportage-/meldproces dient een procedure aanwezig te zijn binnen de gebruikersorganisatie. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het intern rapporteren van de incidenten en waarschuwingen die specifiek zijn voor hun systemen en Azure. Voor dit rapportage-/meldproces dient een procedure aanwezig te zijn binnen de gebruikersorganisatie.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
16.1.2.1	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.	CA-13 CA-16 CA-17 CA-26 CA-29 CA-47	IM - 1 IM - 2 IM - 3 IM - 4 IM - 5 IM - 6	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om vast te stellen of er een meldloket is voor beveiligingsincidenten. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
16.1.2.2	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.	CA-13 CA-16 CA-17 CA-26 CA-29 CA-47	IM - 1 IM - 2 IM - 3 IM - 4 IM - 5 IM - 6	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om op te maken of er een meldprocedure is inclusief taken en verantwoordelijkheden van het meldloket. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Op te maken dat Standard Operating Procedures (SOP's) voor M365-inbreukrespons, M365-beveiligingsincidentrespons-SOP's en incidentresponsplannen aanwezig zijn en dat M365-teams en -personeel vermoedelijke beveiligingsincidenten moeten rapporteren aan het M365-onderzoeks- en responsteam in bijna real- tijd na het ontdekken van een vermoedelijk beveiligingsincident. Hieruit is voor M365 niet expliciet op te maken of een meldprocedure aanwezig is waar in de specifieke taken en verantwoordelijkheden van het meldloket staan beschreven. Azure: Azure heeft de Incident Management SOP ontwikkeld en geïmplementeerd. De SOP voor incidentbeheer biedt Azure een routekaart voor het implementeren van de incidentbeheermogelijkheden. Het doel van de SOP is om begeleiding te bieden met betrekking tot de verantwoordelijkheden van betrokken partijen tijdens elk incident dat de vertrouwelijkheid, integriteit of beschikbaarheid van Azure aantast. De SOP Incident Management legt de verschillende fasen van de levenscyclus van incidentbeheer uit. Details voor elk van de fasen worden toegelicht in het plan. De SOP identificeert ook de interne partners, team overschrijdende contacten, rollen en verantwoordelijkheden, en somt de personen en managementondersteuning op die nodig zijn om de capaciteit voor incidentbeheer effectief te handhaven en te ontwikkelen. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor M365 op te maken dat het M365 Security Incident & Response (SIR)-team gecentraliseerd incidentbeheer en respons voor M365 biedt. Het M365 SIR-team publiceert het M365 Security Incident Response Plan (IR-plan) en een wiki met veel gestelde vragen over beveiligingsincidenten, samen met een "battlecard" met live-incidentinstructies voor M365-personeel. Als onderdeel van de specifieke incidentbeheerprocedures van het serviceteam biedt elk team aanvullende informatie en training om inzicht te krijgen in de verschillende verantwoordelijkheden en		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				verantwoordelijkheden van het team ter ondersteuning van incidentbeheer. Dit is opgenomen onder IR-2 in de M365 FedRAMP-rapportage. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
16.1.2.3	Alle medewerkers en contractanten hebben aantoonbaar kennisgenomen van de meldingsprocedure van incidenten.	CA-13 CA-16 CA-17 CA-26 CA-29 CA-47	IM - 1 IM - 2 IM - 3 IM - 4 IM - 5 IM - 6	Controls aanwezig in FedRAMP-raamwerk Verwachting is dat de meldingsprocedure onderdeel is van het incident management framework is. Echter is niet duidelijk of medewerkers en contracten hiervan kennis hebben genomen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft ontwikkelt, documenteert en verspreidt procedures onder alle relevante personeelsleden of rollen om de implementatie van het incidentresponsbeleid en de bijbehorende beheersmaatregelen voor incidentrespons te vergemakkelijken. Het M365 Risk Management-team heeft de controle over de beveiligingstraining geïmplementeerd door werknemers en contractanten te verplichten om de beveiligings- en bewustzijnstraining jaarlijks te volgen. Niet-operationeel personeel, dat wil zeggen iedereen die betrokken is bij ontwikkeling en kwaliteitsborging, moet ook de verplichte training volgen die wordt aangeboden door Microsoft Online Services Security, evenals training in verband met de operationele procedures met betrekking tot Asset Handling, Incident Response, en Wijzigingsbeheer. Uit bovenstaande is voor M365 niet expliciet op te maken of alle medewerkers en contractanten aantoonbaar kennis hebben genomen van de	Controls aanwezig in ISO control mapping / NIST raamwerk Verwachting is dat de meldingsprocedure onderdeel is van het incident management framework is. Echter is niet duidelijk of medewerkers en contracten hiervan kennis hebben genomen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Azure: Azure-beleid en -procedures worden gedistribueerd en gepubliceerd naar een centrale SharePoint-repository en zijn toegankelijk voor al het Azure-personeel. Het Azure Security Response Team biedt regelmatig updates over gebeurtenistriage en incidentbeheer die beschikbaar zijn voor alle toepasselijke Azure-incidentbeheermedewerkers. Alle Azure-medewerkers hebben een beveiligingsbewustzijnstraining ontvangen, waarbij een incident moet worden gemeld als ze worden blootgesteld aan informatie die niet binnen hun toegewezen toegangsautorisatie valt, en hebben werknemersovereenkomsten (EA's) ondertekend die dienen als geheimhoudingsovereenkomsten (NDA's).	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				meldingsprocedure van incidenten. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor M365 op te maken dat het M365 SIR-team de jaarlijkse beveiligingstraining beoordeelt die wordt gegeven aan al het personeel met toegang tot M365. Er wordt training gegeven aan nieuw en huidig M365-personeel over het detecteren van potentiële incidenten en hoe het onderzoek van die gebeurtenissen over te dragen aan het SIR-team. Dit is opgenomen onder IT-2 in de M365 FedRAMP-rapportage. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor M365 tevens op te maken dat M365 een beveiligingstraining heeft geïmplementeerd voor alle medewerkers, inclusief managers, senior executives en contractanten, en het verplicht is om na e initiële training ten minste jaarlijks een beveiligings- en privacybewustzijnstraining te volgen. Dit is opgenomen onder AT-2 in de M365 FedRAMP-rapportage. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor M365 tevens op te maken dat M365 gebruik maakt van bedrijfstrainingstools om beveiligingstrainingen te documenteren en te bewaken. Bedrijfstrainingstools bieden een rapport dat bijhoudt wie de basisbeveiligingsbewustzijn en specifieke informatiesysteemtraining heeft gevolgd. Dit is opgenomen onder AT-4 in de M365 FedRAMP-rapportage.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
16.1.2.4	Incidenten worden zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld.	CA-13 CA-16 CA-17 CA-26 CA-29 CA-47	IM - 1 IM - 2 IM - 3 IM - 4 IM - 5 IM - 6	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om uit assurance rapportages op te maken of incidenten binnen 24 uur na bekendwording intern worden gemeld. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		zie 16.1.2
16.1.2.5	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.	CA-13 CA-16 CA-17 CA-26 CA-29 CA-47	IM - 1 IM - 2 IM - 3 IM - 4 IM - 5 IM - 6	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om uit assurance rapportages op te maken of de proceseigenaar eindverantwoordelijk is voor het oplossen van beveiligingsincidenten. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het ondersteunen van tijdige reacties op incidenten met het Azure-team.
16.1.2.6	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.	CA-13 CA-16 CA-17 CA-26 CA-29 CA-47	IM - 1 IM - 2 IM - 3 IM - 4 IM - 5 IM - 6	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om uit assurance rapportages op te maken of de opvolging van incidenten maandelijks wordt gerapporteerd aan de verantwoordelijke. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		
16.1.2.7	Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD) procedure is onderdeel van de incidentrapportage.	CA-13 CA-16 CA-17 CA-26 CA-29 CA-47	IM - 1 IM - 2 IM - 3 IM - 4 IM - 5 IM - 6	Controls aanwezig in FedRAMP-raamwerk Het is niet mogelijk om uit assurance rapportages op te maken of informatie uit de CVD-procedure onderdeel is van de incidentrapportage. Uit aanvullende ontvangen FedRAMP-rapportages (geen assurance) is voor M365 op te maken dat M365 gebruik maakt van penetratietesten en een bug bounty programma om privé-informatie te identificeren die openbaar beschikbaar is. Als er niet-openbare informatie wordt geïdentificeerd als onderdeel van dit proces, wordt het Microsoft M365-	Geen controls beschreven Het is niet mogelijk om uit assurance rapportages op te maken of informatie uit de CVD-procedure onderdeel is van de incidentrapportage. Ook voor Azure is online op te maken dat een bug bounty programma opgezet (https://www.microsoft.com/en-us/msrc/bounty-microsoft-azure). Hieruit is niet op te maken of de informatie afkomstig uit de CVD-procedure onderdeel is van de incident rapportage.	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				incidentresponsproces gevolgd om het probleem te onderzoeken en op te lossen. Hieruit is niet op te maken of de informatie afkomstig uit de CVD-procedure onderdeel is van de incident rapportage. Dit is opgenomen onder RA-5 in de M365 FedRAMP-rapportage.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging: Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren	CA-27 CA-45	SOC2 - 6 SOC2 - 9	Controls aanwezig in ISO control mapping / NIST raamwerk Rapportage van zwakke plekken door medewerkers en contractanten niet expliciet in assurance rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. Microsoft vereist dat werknemers en contractanten die de M365-informatiesystemen en -services van de organisatie gebruiken, waargenomen of vermoede zwakke punten in de informatiebeveiliging in systemen of services opmerken en rapporteren. Werknemers en contractanten van Microsoft zijn verplicht om waargenomen of vermoede zwakke punten in de informatiebeveiliging in systemen of services op te merken en te melden. M365-beveiligingsincidenten, zwakke punten en storingen moeten onmiddellijk worden gemeld door Microsoft en personeel van aannemers. De rapportage en afhandeling van deze gebeurtenissen volgen voorgeschreven procedures volgens een gedefinieerd en geïmplementeerd incidentresponsbeleid.	Controls aanwezig in FedRAMP-raamwerk Rapportage van zwakke plekken door medewerkers en contractanten niet expliciet in assurance rapportage. Uit aanvullende ontvangen FedRAMP-rapportage (geen assurance) is voor Azure op te maken dat van alle personeelsleden wordt geëist dat zij gebeurtenissen onmiddellijk melden wanneer ze geloven dat er een beveiligingsincident heeft plaatsgevonden. Voorbeelden van dergelijke gebeurtenissen omvatten, maar zijn niet beperkt tot: * Waarschuwingen, meldingen, foutmeldingen of andere geautomatiseerde waarschuwingen die wijzen op een beveiligingsincident kan hebben plaatsgevonden. * Meldingen van beveiligingsincidenten ontvangen van externe partijen, waaronder klanten, leden van de pers of het grote publiek. Personeel kan incidenten melden door gebeurtenis gerelateerde gegevens handmatig in te voeren in het ticketingsysteem voor incidentbeheer. Dit is opgenomen onder IR-06 in de Azure FedRAMP-rapportage.	M365 - CUEC-08: De gebruikersorganisaties is verantwoordelijk voor het melden van geïdentificeerde beveiligings-, beschikbaarheids-, verwerkingsintegriteits - en vertrouwelijkheidsproblemen. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het aan Microsoft rapporteren van de incidenten en waarschuwingen die specifiek zijn voor hun systemen en Azure. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het onmiddellijk op de hoogte stellen van de MFA-service van feitelijke of vermoedelijke inbreuken op de informatiebeveiliging, inclusief gecompromitteerde gebruikers-accounts.
16.1.3.1	Een Coordinated Vulnerability Disclosure (CVD) procedure is gepubliceerd en ingericht.	CA-27 CA-45	SOC2 - 6 SOC2 - 9	Ontbreken control in SOC geaccepteerd door werkgroep. Uit assurance rapportages van Azure en M365 is niet op te maken dat een CVD is gepubliceerd en ingericht. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit		Zie 16.1.3

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Hieruit is niet op te maken of een CVD procedure is gepubliceerd en ingericht. Per interview met Microsoft en op basis van de Microsoft website met betrekking tot de 'Microsoft Bug Bounty Program' (https://www.microsoft.com/en-us/msrc/bounty) is op te maken dat een Coordinated Vulnerability Disclosure procedure is gepubliceerd en ingericht. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien uit aanvullende informatie blijkt dat een publiekelijk toegankelijk bug bounty programma aanwezig is voor het indienen van CVD meldingen.		
16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	CA-13 CA-17 CA-26 CA-29 CA-47	SOC2 - 9 IM - 1 IM - 2 IM - 3 IM - 6 VM - 4	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Algemeen - CUEC: De gebruikersorganisatie is verantwoordelijk voor het inrichten van een proces om een door Microsoft aan hen gemeld security incident met het NCSC te delen.
16.1.4.1	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatieverwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT.	CA-13 CA-17 CA-26 CA-29 CA-47	SOC2 - 9 IM - 1 IM - 2 IM - 3 IM - 6 VM - 4	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om uit assurance rapportages op te maken dat dergelijke incidenten binnen 72 uur worden gemeld aan NCSC of sectorale CERT. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft reageert op M365-informatiebeveiligingsincidenten in overeenstemming met de gedocumenteerde procedures. Microsoft heeft robuuste processen voor M365 ontwikkeld om een gecoördineerde reactie op incidenten te vergemakkelijken als zich een incident zou voordoen. Het Microsoft Security Incident Response-proces voor M365 is onderverdeeld in de volgende fasen: - Identificatie: systeem- en beveiligingswaarschuwingen kunnen worden verzameld, gecorreleerd en geanalyseerd. Gebeurtenissen worden onderzocht door M365-operaties en beveiligingsorganisaties. Als een gebeurtenis wijst op een beveiligingsprobleem, krijgt het incident een ernstclassificatie toegewezen en wordt het op de juiste manier geëscaleerd. Deze escalatie omvat product-, beveiligings- en engineeringspecialisten. - Containment: Het escalatieteam evalueert de omvang en impact van een incident. De directe		Zie 16.1.4

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				prioriteit van het escalatieteam is ervoor te zorgen dat het incident wordt ingeperkt en dat de gegevens veilig zijn. - Uitroeiing: nadat de situatie onder controle is, gaat het escalatieteam verder met het uitroeien van eventuele schade veroorzaakt door de beveiligingsinbreuk en identificeert het de hoofdoorzaak waarom het beveiligingsprobleem zich heeft voorgedaan. Als een kwetsbaarheid wordt vastgesteld, meldt het escalatieteam het probleem aan de productengineering. - Herstel: tijdens herstel worden software- of configuratie-updates toegepast op het systeem en worden services weer volledig operationeel. - Geleerde lessen: elk beveiligingsincident wordt geanalyseerd om ervoor te zorgen dat de juiste mitigaties worden toegepast om te beschermen tegen toekomstige herhalingen. Azure: Azure rapporteert bevestigde beveiligings- en beschikbaarheidsincidenten aan DoD, US-CERT en getroffen klanten in overeenstemming met de toepasselijke beleidsregels en procedures. Het Azure Security-team coördineert met de ISSO om de juiste overheidscontacten op de hoogte te stellen, inclusief, indien van toepassing, autoriserende functionarissen, overheidsklanteninstanties, US-CERT, en anderen, van een incident, incidentupdates en oplossing. Azure rapporteert gebeurtenissen met federale gegevens volgens de tijdlijnen en het proces zijn gedocumenteerd in de Incident Management SOP. De SOP identificeert de soorten beveiligingsincidenten die moeten worden gemeld aan de federale overheid, rapportagetermijnen en specifieke processen voor het rapporteren en afhandelen van incidenten waarbij federale klantgegevens betrokken zijn. Hieruit is niet op te maken of de relevante informatiebeveiligingsincidenten binnen 72 uur gemeld worden. Uit de: 'Bijlage Bescherming van persoonsgegevens voor Producten en Diensten van Microsoft' (laatst bijgewerkt op 15-09-2021) is op te maken dat "Voor elke schending van de beveiliging die een Beveiligingsincident inhoudt, wordt door Microsoft zonder onnodige vertraging, en in elk geval binnen 72 uur, een kennisgeving verstrekt (zoals beschreven in de sectie “Kennisgeving van Beveiligingsincidenten” hierboven)." De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
16.1.5	Respons op informatiebeveiligingsincidenten: Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	CA-13 CA-17 CA-26 CA-29 CA-47	IM - 1 IM - 2 IM - 3 IM - 6 VM - 4	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het aan Microsoft rapporteren van de incidenten en waarschuwingen die specifiek zijn voor hun systemen en Azure. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het ondersteunen van tijdige reacties op incidenten met het Azure-team.
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
16.1.6	Lering uit informatiebeveiligingsincidenten: Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	n.v.t.	IM - 4 IM - 5	Controls aanwezig in ISO control mapping / NIST raamwerk Lering uit dergelijke incidenten is niet expliciet benoemd in de assurance rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. Hieruit is op te maken dat Microsoft kennis gebruikt die is opgedaan bij het analyseren en oplossen van informatiebeveiligingsincidenten om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
16.1.6.1	Beveiligingsincidenten worden geanalyseerd met als doel te leren en toekomstige beveiligingsincidenten te voorkomen.	n.v.t.	IM - 4 IM - 5	Controls aanwezig in ISO control mapping / NIST raamwerk Lering uit dergelijke incidenten is niet expliciet benoemd in de assurance rapportages. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft gebruikt kennis die is opgedaan bij het analyseren en oplossen van informatiebeveiligingsincidenten om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen. Microsoft correleert incidentinformatie en individuele incidentreacties om een organisatiebreed perspectief te krijgen op incidentbewustzijn en -respons. De M365-service- en platformteams, het beveiligingsteam en het M365 Security Incident Response (SIR)-team zijn verantwoordelijk voor het beheer van het onderzoek en de oplossing van beveiligingsincidenten binnen M365. Het M365-beveiligingsteam en het M365 SIR-team werken samen met andere teams om ervoor te zorgen dat beveiligingsincidenten worden ingeperkt, uitgeroeid en dat het herstel wordt voltooid. De Product Marketing Group werkt samen met andere teams om klanten op de hoogte te stellen van beveiligingsincidenten, waar van toepassing, en om het proces voor het reageren op privacy-incidenten te starten als er bezorgdheid bestaat dat er mogelijk een inbreuk op de privacy heeft plaatsgevonden. De M365 SIR-teamleider en -onderzoeker zullen alle belangrijke details van de reactie op beveiligingsincidenten die uit hun onderzoek voortvloeien, opnemen en ervoor zorgen dat deze op de juiste manier worden weergegeven met registratietools. Azure: Als onderdeel van IcM moeten serviceteams, wanneer een incident is opgelost, een oplossing bieden. Wanneer het incident is verholpen, lost het serviceteam met het toegewezen incidentticket het incident op en geeft het de maatregelen die zijn genomen om het incident op te lossen. Serviceteams kunnen ook root cause-informatie aanleveren om eventueel de incidenten binnen IcM te correleren. Voor alle incidenten met ernstgraad 0, 1 of 2 wordt een Post Incident Response (PIR)-beoordeling uitgevoerd door het Security Response Team om de details van de hoofdoorzaak vast te stellen en een rapport op te stellen met alle lessen die uit het incident zijn getrokken. Het doel van deze beoordelingen is om: - Identificeer technische of communicatiefouten, procedurefouten, handmatige fouten, procesfouten die mogelijk het Beschikbaarheidsincident hebben veroorzaakt of die zijn geïdentificeerd met een formele PIR - Zorg ervoor dat technische fouten worden vastgelegd en kunnen worden opgevolgd met technische teams in de vorm van bugs in hun operationele databases - Evalueren van reactieprocedures op toereikendheid en volledigheid van operationele procedures. Hieruit is op te maken dat beveiligingsincidenten worden geanalyseerd met als doel om hiervan te leren en in het vervolg te voorkomen.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
16.1.6.2	De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen.	n.v.t.	IM - 4 IM - 5	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om uit assurance rapportages op te maken of relevante partners worden geïnformeerd. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien het wel beoordelen van deze uitgangspunten in de overheidsmaatregel geen aanvullende zekerheid geeft betreffende de bovenliggende BIO-control.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
16.1.7	Verzamelen van bewijsmateriaal: De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	n.v.t.	CCM - 9	Controls aanwezig in ISO control mapping / NIST raamwerk Verzameling van bewijsmateriaal is niet expliciet benoemd in de assurance rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. Microsoft definieert en past procedures toe voor de identificatie, verzameling, verwerving en bewaring van informatie, die als bewijs kan dienen. Microsoft implementeert een mogelijkheid voor het afhandelen van incidenten voor beveiligingsincidenten, waaronder voorbereiding, detectie en analyse, inperking, uitroeiing en herstel. Microsoft neemt elk beveiligingsincident zeer serieus. Wanneer Microsoft zich bewust wordt van een beveiligingsincident, gebruikt Microsoft een gedefinieerd reactieproces voor beveiligingsincidenten, inclusief forensisch onderzoek, om precies bij te houden wat er is gebeurd, welke gegevens zijn geopend en door wie. De teamleider en onderzoeker van het Security Incident Response-team nemen alle significante details die voortvloeien uit het onderzoek op in het registratiesysteem. Hieruit is op te maken dat procedures aanwezig zijn en toegepast worden voor het verzamelen van bewijsmateriaal.	Controls aanwezig in assurance rapportage (SOC)	Algemeen - CUEC: De gebruikersorganisaties is verantwoordelijk voor het definiëren en toepassen van procedures voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen in geval van een (vermoed) informatiebeveiligings-incident.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
16.1.7.1	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.	n.v.t.	CCM - 9	Controls aanwezig in FedRAMP-raamwerk Het is niet mogelijk om op te maken wat de bewaartermijn van gelogde incidentinformatie is. Tevens wordt verzameling van bewijsmateriaal niet expliciet benoemd in de M365 rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft definieert en past procedures toe voor de identificatie, verzameling, verwerving en bewaring van informatie, die als bewijs kan dienen. Microsoft implementeert een mogelijkheid voor incidentafhandeling voor beveiligingsincidenten, waaronder voorbereiding, detectie en analyse, inperking, uitroeiing en herstel. Microsoft neemt elk beveiligingsincident zeer serieus. Zodra Microsoft zich bewust wordt van een beveiligingsincident, gebruikt Microsoft een gedefinieerd reactieproces voor beveiligingsincidenten, inclusief forensisch onderzoek, om precies bij te houden wat er is gebeurd, welke gegevens zijn geopend en door wie. De teamleider en onderzoeker van het Security Incident Response-team nemen alle significante details die voortvloeien uit het onderzoek op in het registratiesysteem. Azure: Azure behandelt het incidentbeheerbeleid als onderdeel van het Microsoft-beveiligingsbeleid, waarvan er twee sets zijn: het Microsoft Security Policy (MSP) dat van toepassing is op al het personeel, en het Microsoft Security Program Policy (MSPP), dat van toepassing is aan al het personeel dat verantwoordelijk is voor de beveiliging. De Microsoft Information Risk Management Council (IRMC) is het bestuursorgaan met beoordelings- en goedkeuringsverantwoordelijkheid voor de MSP en MSPP. Binnen Azure is de MSPP specifiek van toepassing op al het personeel dat betrokken is bij het ontwerpen, bouwen en exploiteren van Azure en op alle informatie en processen die worden gebruikt bij het uitvoeren van Microsoft-activiteiten. Alle Azure-medewerkers zijn verantwoordelijk en verantwoordelijk voor de naleving van deze leidende principes binnen hun toegewezen rollen. Het beleid richt zich op; incidentbeheer, procedures en training, incidentbewijs en incident managementcapaciteiten. Hieruit is niet op te maken wat de bewaartermijn is van gelogde incidentinformatie in geval van een (vermoed) beveiligingsincident. Uit aanvullend ontvangen FedRAMP-rapportages is op te maken dat audit records minimaal één jaar worden bewaard. Dit is opgenomen in AU-11 van de Azure en M365 FedRAMP-rapportages.		Algemeen - CUEC: De gebruikersorganisatie is verantwoordelijk voor het opslaan van relevante data in geval van een (vermoed) informatiebeveiligings-incident.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
17.1.1	Informatiebeveiligingscontinuïteit plannen: De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen.	ELC-09	BC - 1 BC - 3 BC - 7 BC - 8	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het ontwikkelen van hun eigen Disaster Recovery Plan en Business Continuity Plan om te kunnen omgaan met situaties waarin het niet mogelijk is om toegang te krijgen tot of gebruik te maken van MFA-services.
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.
17.1.2	Informatiebeveiligingscontinuïteit implementeren: De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	ELC-09 CA-50	BC - 1 BC - 3 BC - 7 BC - 8	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het ontwikkelen van hun eigen Disaster Recovery Plan en Business Continuity Plan om te kunnen omgaan met situaties waarin het niet mogelijk is om toegang te krijgen tot of gebruik te maken van MFA-services.
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren: De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	ELC-09 CA-50	BC - 1 BC - 3 BC - 4 BC - 5 BC - 6 BC - 7 BC - 8 BC - 9	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
17.1.3.1	Continuïteitsplannen worden jaarlijks getest op geldigheid en bruikbaarheid.	ELC-09 CA-50	BC - 1 BC - 3 BC - 4 BC - 5 BC - 6 BC - 7 BC - 8 BC - 9	Controls aanwezig in ISO control mapping / NIST raamwerk Voor M365 Het is niet mogelijk om uit assurance rapportages op te maken hoe vaak deze plannen worden getest. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. Hieruit is op te maken dat de noodplannen (continuïteitsplannen) minimaal jaarlijks worden getest om ervoor te zorgen dat de controles aanwezig zijn en naar behoren functioneren.	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
17.1.3.2	Door het uitvoeren van een expliciete risicoafweging worden de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd.	ELC-09 CA-50	BC - 1 BC - 3 BC - 4 BC - 5 BC - 6 BC - 7 BC - 8 BC - 9	Controls aanwezig in ISO control mapping / NIST raamwerk Voor M365 Het is niet mogelijk om uit assurance rapportages op te maken op welke basis de criticality is bepaald. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. M365: Microsoft ontwikkelt een noodplan voor het informatiesysteem dat essentiële missies en zakelijke functies en bijbehorende noodvereisten identificeert. Microsoft heeft een speciaal Business Continuity Management (BCM)-team dat ondersteuning biedt om M365-teams te helpen bij het analyseren van continuïteits- en noodherstelvereisten, het documenteren van procedures en het testen van vastgestelde procedures. Hieruit is op te maken dat de plannen en betrouwbaarheidseisen worden vastgesteld op basis van het identificeren van essentiële missies en zakelijke functies. Hierbij is echter niet expliciet op te maken dat een risico-afweging wordt uitgevoerd.	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
17.1.3.3	De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten uiterlijk binnen een week hersteld.	ELC-09 CA-50	BC - 1 BC - 3 BC - 4 BC - 5 BC - 6 BC - 7 BC - 8 BC - 9	Controls aanwezig in ISO control mapping / NIST raamwerk Het is niet mogelijk om op te maken wat de remediation timelines zijn voor zowel M365 als Azure. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft ontwikkelt een noodplan voor het informatiesysteem dat hersteldoelstellingen, herstelprioriteiten en metrische gegevens biedt. Microsoft handhaaft een raamwerk dat consistent is met best practices uit de branche en dat het continuïteitsprogramma op niveaus stimuleert. Het raamwerk omvat: - Toewijzing van de belangrijkste resourceverantwoordelijkheden - Meldings-, escalatie- en aangifteprocessen - Hersteltijddoelen en herstelpuntdoelen (RTO en RPO) - Continuïteitsplannen met gedocumenteerde procedures - Trainingsprogramma voor het voorbereiden van de juiste partijen om het Continuïteitsplan uit te voeren - Een test-, onderhouds- en revisieproces Azure: Azure-plannen voor de hervatting van essentiële services binnen de Recovery Time Objective (RTO) van elke service, gedefinieerd door de Business Impact Analysis (BIA) binnen de service specifieke plannen. Essentiële diensten worden gedefinieerd als diensten met een RTO van 168 uur of minder. Hieruit is op te maken dat zowel voor M365 als voor Azure een RTO is opgesteld. Hierbij is echter wel op te maken dat de RTO van Azure op 1 week of minder is gesteld voor essentiële diensten, echter is voor M365 niet op te maken wat de specifieke gestelde tijdslijnen zijn.		Algemeen - CUEC: De gebruikersorganisaties is verantwoordelijk voor de eigen inrichting van de configuraties omtrent continuïteit.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten: Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	n.v.t.	BBC - 4 BC - 7 BC - 8 DS - 6 DS - 7	Controls aanwezig in ISO control mapping / NIST raamwerk Beschikbaarheid van informatieverwerkende faciliteiten niet expliciet op te maken uit assurance rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. Alle serviceteams gebruiken capaciteitsplanning als een belangrijk kenmerk van hun datacentermodellen en datareplicatieplannen om ervoor te zorgen dat er voldoende capaciteit is voor informatieverwerking, telecommunicatie en omgevingsondersteuning. Er zijn actieve alternatieve locaties voor elk serviceteam. Alle alternatieve sites zijn actieve sites die gebruikmaken van bijna realtime gegevensreplicatie. Elke alternatieve site is redundant en wordt beheerd door Azure. De herstelafspraken met Azure zijn in overeenstemming met de hersteltijddoelstellingen die zijn vastgelegd in de Business Impact Analyse van de serviceteams. Alternatieve opslaglocaties hebben fysieke beveiligingsmaatregelen die gelijkwaardig zijn aan die van de primaire locatie. Hieruit is op te maken dat informatieverwerkende faciliteiten met redundantie worden geïmplementeerd.	Controls aanwezig in assurance rapportage (SOC)	
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
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 informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.	CA-07 CA-12 CA-25 ELC-15	ELC - 2 SOC2 - 18 SOC2 - 19 SOC2 - 25	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor de naleving van toepasselijke wet-/regelgeving. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het begrijpen en naleven van de inhoud van hun servicecontracten, inclusief verplichtingen met betrekking tot systeembeveiliging, beschikbaarheid, verwerkingsintegriteit en vertrouwelijkheid.
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
18.1.2	Intellectuele-eigendomsrechten: Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen behoren passende procedures te worden geïmplementeerd.	n.v.t.	n.v.t.	Ontbreken control in SOC geaccepteerd door werkgroep. Intellectuele eigendomsrechten niet expliciet opgenomen in rapportages. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. Microsoft implementeert passende procedures om te zorgen voor naleving van wettelijke, regelgevende en contractuele vereisten met betrekking tot intellectuele eigendomsrechten en het gebruik van prioritaire softwareproducten. Microsoft gebruikt software en bijbehorende documentatie in overeenstemming met contractovereenkomsten en auteursrechtwetten. Risico's verbonden aan schendingen van intellectuele eigendomsrechten worden meegewogen in de technische en procedurele controles die van toepassing zijn op het serviceaanbod van Microsoft. De overgrote meerderheid van de software die wordt gebruikt om services te leveren, is echter de M365-suite van Microsoft. Hieruit is op te maken dat procedures omtrent intellectuele eigendomsrechten zijn geïmplementeerd. De werkgroep heeft risicogebaseerd aangegeven dat voor deze control geen aanvullende verduidelijking of assurance benodigd is aangezien intellectuele eigendomsrechten onder de verantwoordelijkheid van de gebruikersorganisatie vallen.	Ontbreken control in SOC geaccepteerd door werkgroep. Intellectuele eigendomsrechten niet expliciet opgenomen in rapportages. Uit aanvullend ontvangen FedRAMP-rapportage (geen assurance) is voor Azure op te maken dat interne software die binnen de Azure-grens wordt gebruikt, is ontwikkeld door Microsoft en is daarom niet onderworpen aan contractuele vereisten, auteursrechtbeperkingen en licentiebewaking voor naleving van relaties met derden. In overeenstemming met de Third Party Software Policy, moet alle software van derden worden gekocht via een bedrijfsfunctie om het volgen van alle software-aankopen, naleving van softwarelicentievoorwaarden en bedrijfsrisicovermindering door blootstelling aan licentieovereenkomsten mogelijk te maken. Microsoft voldoet aan alle vereisten voor softwaregebruik zoals gedefinieerd in de contractuele overeenkomst met de leverancier. Dit is opgenomen onder CM-10 in de Azure FedRAMP-rapportage. De werkgroep heeft risicogebaseerd aangegeven dat voor deze control geen aanvullende verduidelijking of assurance benodigd is aangezien intellectuele eigendomsrechten onder de verantwoordelijkheid van de gebruikersorganisatie vallen.	Algemeen - CUEC: De gebruikersorganisaties is verantwoordelijk voor het gebruik van software en bijbehorende documentatie in overeenstemming met contractovereenkomsten en auteursrechtwetten. Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor het begrijpen en naleven van de inhoud van hun servicecontracten, inclusief verplichtingen met betrekking tot systeembeveiliging, beschikbaarheid, verwerkingsintegriteit en vertrouwelijkheid.
	Geen (aanvullende) maatregelen voor overheidsinstanties.	n.v.t	n.v.t	n.v.t	n.v.t	n.v.t.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
18.1.3	Beschermen van registraties: Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	CA-55 ELC-08	SOC2 - 13 SOC2 - 14 DS - 15	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor de naleving van toepasselijke wet- /regelgeving.
18.1.3.1	De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.	CA-55 ELC-08	SOC2 - 13 SOC2 - 14 DS - 15	Ontbreken control in SOC geaccepteerd door werkgroep. Het is niet mogelijk om op te maken dat per soort informatie door de proceseigenaar inzichtelijk is gemaakt wat de bewaartermijn is. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft beschermt records tegen verlies, vernietiging, vervalsing, ongeoorloofde toegang en ongeoorloofde vrijgave, in overeenstemming met wettelijke, regelgevende, contractuele en zakelijke vereisten. Microsoft handhaaft verplicht toegangscontrolebeleid voor onderwerpen en objecten waarbij het beleid specificeert dat een onderwerp dat toegang heeft gekregen tot informatie, de informatie niet mag doorgeven aan niet-geautoriseerde onderwerpen of objecten. M365-activa die eigendom zijn van Microsoft worden behouden zoals van toepassing op basis van de bewaarvereisten die zijn vastgesteld door het Corporate Records Managementteam van Microsoft en de classificatie van een bedrijfsmiddel, of op basis van contractuele vereisten. Azure: alle informatie waarvan een back-up is gemaakt en die is opgeslagen, maakt gebruik van de gegevenstypeclassificatie volgens CELA-gegevensclassificatie. Serviceteams moeten de gegevenstypeclassificatie identificeren die op zijn beurt het toegewezen retentie- en opslagbeleid aanstuurt. Uit bovenstaande is op te maken dat bewaartermijn en -vereisten worden vastgesteld op basis van de gegevensclassificatie/classificatie van een bedrijfsmiddel. Hieruit is op te maken dat voor verschillende soorten informatie (met verschillende classificaties) specifieke eisen zijn opgesteld. Hieruit is echter niet op te maken wat de specifiek bewaartermijnen zijn. Uit aanvullend ontvangen FedRAMP-rapportages is op te maken dat audit records minimaal één jaar worden bewaard. Microsoft garandeert de bewaring van tenant gegevens gedurende 30 dagen na beëindiging van de diensten en alle informatie wordt 90 dagen na beëindiging van de service permanent verwijderd. Het Microsoft-documentatieretentiebeleid van Corporate Records Management beschrijft welke Microsoft-documenten moeten worden		Algemeen - CUEC: De gebruikersorganisaties is verantwoordelijk voor het inzichtelijk maken van de bewaartermijn voor de (verschillende soorten) informatie van de gebruikersorganisatie.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				bewaard en voor hoe lang. Dit is opgenomen in AU-11 en SI-12 van de Azure en M365 FedRAMP-rapportages. De werkgroep heeft risicogebaseerd aangegeven dat voor deze overheidsmaatregel geen aanvullende verduidelijking of assurance benodigd is, aangezien de beheersmaatregel specifiek cliënt data betreft, waarbij de klant derhalve verantwoordelijk is voor het inzichtelijk maken van de bewaartermijn.		
18.1.4	Privacy en bescherming van persoonsgegevens: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	n.v.t.	n.v.t.	Ontbreken control in SOC geaccepteerd door werkgroep. Privacy en bescherming van persoonsgegevens niet expliciet opgenomen in assurance rapportages. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft zorgt voor de bescherming en privacy van persoonlijk identificeerbare informatie zoals vereist in relevante wet- en regelgeving, indien van toepassing. Microsoft bepaalt en documenteert de wettelijke autoriteit die het verzamelen, gebruiken, onderhouden en delen van persoonlijk identificeerbare informatie (PII) toestaat, in het algemeen of ter ondersteuning van een specifiek programma of informatiesysteem. Azure: Microsoft heeft een team van privacymanagers die toezicht houden op heel Azure om ervoor te zorgen dat privacywetten en -regelgeving in overeenstemming zijn met het bestuur met betrekking tot persoonlijk identificeerbare informatie. Hieruit is op te maken dat privacy en bescherming van persoonsgegevens wordt gewaarborgd in overeenstemming met relevante wet- en regelgeving. De werkgroep heeft risicogebaseerd aangegeven dat voor deze control geen aanvullende verduidelijking of assurance benodigd is aangezien privacy en bescherming van persoonsgegevens onder de verantwoordelijkheid van de gebruikersorganisatie vallen.		Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor de naleving van toepasselijke wet-/regelgeving.

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
18.1.4.1	In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.	n.v.t.	n.v.t.	Controls aanwezig in ISO control mapping / NIST raamwerk De FG / Data Protection Officer en AVG / GDPR worden niet expliciet genoemd in de assurance rapportages. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft zorgt voor de bescherming en privacy van persoonlijk identificeerbare informatie zoals vereist in relevante wet- en regelgeving, indien van toepassing. Azure: Microsoft onderhoudt een team van privacymanagers die toezicht houden op heel Azure om ervoor te zorgen dat privacywetten en -regelgeving in overeenstemming zijn met governance met betrekking tot persoonlijk identificeerbare informatie.		Algemeen - CUEC: De gebruikersorganisaties is verantwoordelijk voor het binnen de eigen organisatie aanstellen van een Functionaris Gegevens-bescherming met voldoende mandaat om zijn/haar functie uit te voeren.
18.1.4.2	Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	n.v.t.	n.v.t.	Controls aanwezig in ISO control mapping / NIST raamwerk De FG / Data Protection Officer en AVG / GDPR worden niet expliciet genoemd in de assurance rapportages. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. M365: Microsoft zorgt voor de bescherming en privacy van persoonlijk identificeerbare informatie zoals vereist in relevante wet- en regelgeving, indien van toepassing. Microsoft bepaalt en documenteert de wettelijke autoriteit die het verzamelen, gebruiken, onderhouden en delen van persoonlijk identificeerbare informatie (PII) toestaat, in het algemeen of ter ondersteuning van een specifiek programma of informatiesysteem. Activa die eigendom zijn van M365 worden behouden zoals van toepassing op basis van bewaarvereisten die zijn vastgesteld door het Corporate Records Managementteam van Microsoft en de classificatie van activa, of op basis van contractuele vereisten. De classificatie van assets is opgenomen in de M365-assetinventaris. Microsoft gebruikt een uitgebreid raamwerk om te voldoen aan FISMA, SSAE 16, HIPAA, ISO 27011 en andere voorschriften waar nodig. Als onderdeel van dit raamwerk onderhoudt Microsoft doorlopende continue monitoringprogramma's om te zorgen voor M365-compliance bij postproductie-implementaties. Azure: Microsoft handhaaft het Microsoft-privacybeleid en de eindgebruikerslicentie en openbare sites met juridische kennisgevingen, waaronder de Microsoft-privacyverklaring. In deze privacyverklaring documenteert Microsoft het doel, de verzameling, het gebruik, het onderhoud en het delen van de informatie die ze verzamelen. Microsoft communiceert zijn privacyverplichtingen aan externe entiteiten via licentievoorwaarden in de Online Services Terms (OST) en Online Services Data Protection Addendum (DPA), en de Microsoft Privacyverklaring. Alle services binnen Azure zijn onderworpen aan een privacybeoordeling.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				Privacymanagers zijn verantwoordelijk voor het beoordelen en goedkeuren van nieuwe diensten op basis van de data-inventarisatie en datagevoeligheid. Juridisch personeel van Microsoft controleert alle verzamelde PII om er zeker van te zijn dat er een wettelijke bevoegdheid bestaat om de informatie te verzamelen. Microsoft heeft ook een Privacy Impact Assessment (PIA) voltooid als onderdeel van het beveiligingsbeoordelingsproces, beschikbaar als onderdeel van het Azure-pakket. Uit bovenstaande is op te maken dat zowel voor M365 als voor Azure maatregelen zijn getroffen omtrent de naleving van privacyregels en informatieverwerking en -procedures.		
18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen: Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	n.v.t.	DS-4	Controls aanwezig in ISO control mapping / NIST raamwerk Voorschriften voor het gebruik van cryptografische beheersmaatregelen niet expliciet opgenomen in assurance rapportages. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Microsoft gebruikt cryptografische controles in overeenstemming met relevante overeenkomsten, wet- en regelgeving. Microsoft implementeert mechanismen voor authenticatie naar een cryptografische module die voldoen aan de vereisten van toepasselijke federale wetten, uitvoeringsbesluiten, richtlijnen, beleid, voorschriften, normen en richtlijnen voor dergelijke authenticatie. Azure implementeert cryptografie via versleutelingsmechanismen en -technieken volgens de vereisten die zijn beschreven in de cryptografische controles van het Microsoft Security Program Policy (MSPP). FIPS 140-2 gevalideerde cryptografische modules worden gebruikt om de naleving van federale wetten, uitvoeringsbesluiten, richtlijnen, beleid, voorschriften en normen te ondersteunen. Uit bovenstaande is op te maken dat voorschriften voor het gebruik van cryptografische beheersmaatregelen aanwezig zijn om deze maatregelen toe te passen in overeenstemming met relevante overeenkomsten, wet- en regelgeving.		Azure - CUEC: De gebruikersorganisatie is verantwoordelijk voor de naleving van toepasselijke wet-/regelgeving.
18.1.5.1	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de ‘pas toe of leg uit’-lijst van het Forum.	n.v.t.	DS-4	Controls aanwezig in ISO control mapping / NIST raamwerk De standaarden zoals in de lijst van het Forum zijn niet expliciet opgenomen in de assurance rapportages. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Op basis van de uitgevoerde werkzaamheden is niet expliciet op te maken of alle cryptografische beheersmaatregelen aansluiten bij de 'pas toe of leg uit'-lijst van het Forum. Wel is op te maken dat Azure o.a. gebruik maakt van IPv4 en IPv6, en TLS1.2. Tevens is voor M365 op te maken dat gebruikt wordt gemaakt van FIPS 140-2 modules en ciphers.		

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
18.2.1	Onafhankelijke beoordeling van informatiebeveiliging: De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.	CA-07 CA-11 CA-25 ELC-04 ELC-11 ELC-15	SOC2 - 20 SOC2 - 27 ELC - 5	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
18.2.1.1	Er is een information security management system (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt.	CA-07 CA-11 CA-25 ELC-04 ELC-11 ELC-15	SOC2 - 20 SOC2 - 27 ELC - 5	Controls aanwezig in ISO control mapping / NIST raamwerk In de M365 assurance rapportage wordt niet expliciet gesproken over een ISMS. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. M365: Microsoft plant, implementeert en controleert de processen die nodig zijn om te voldoen aan de informatiebeveiligingsvereisten en om de acties te implementeren die zijn bepaald in het M365 Information Security Management System (ISMS). Bij het plannen van het M365 Information Security Management System (ISMS) houdt Microsoft rekening met de problemen waarnaar wordt verwezen in het ISMS en de vereisten waarnaar wordt verwezen in het ISMS en bepaalt het de risico's en kansen die moeten worden aangepakt om ervoor te zorgen dat het ISMS zijn beoogde doel kan bereiken. Onder leiding van het M365 Risk and Remediation managementteam volgt Microsoft een gevestigde benadering van risicobeheer en voert minimaal elk fiscaal jaar een jaarlijkse wereldwijde risicobeoordeling uit. Het doel van	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				risicobeoordelingen is het identificeren en prioriteren van de specifieke strategische en operationele risico's van elke divisie op basis van impact, waarschijnlijkheid en managementcontrole en om ervoor te zorgen dat het ISMS de beoogde uitkomst(en) kan bereiken. Risicobeoordelingen zijn ook gericht op het identificeren en uitvoeren van proactieve acties om ongewenste effecten te voorkomen of te verminderen en om continue verbetering te bereiken. Uit bovenstaande is op te maken dat binnen M365 de PDCA-cyclus wordt doorlopen door middel van de processen die zijn ingericht in en omtrent het ISMS.		
18.2.1.2	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	CA-07 CA-11 CA-25 ELC-04 ELC-11 ELC-15	SOC2 - 20 SOC2 - 27 ELC - 5	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	
18.2.2	Naleving van beveiligingsbeleid en -normen: De directie behoort regelmatig de naleving van de informatieverwerking en - procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	CA-02 CA-07 CA-10 CA-53 ELC-04	SOC2 - 19 SOC2 - 20 ELC - 2 ELC - 5	Controls aanwezig in ISO control mapping / NIST raamwerk Beoordeling van de naleving van beveiligingsbeleid en -normen niet expliciet opgenomen in assurance rapportage. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportage (geen assurance) over ISO27001-certificering (2016) voor M365. Het managementteam van M365 beoordeelt regelmatig of de informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied voldoen aan het juiste beveiligingsbeleid, de juiste normen en andere beveiligingsvereisten. M365 beoordeelt en actualiseert regelmatig de huidige controle-	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
				en verantwoordingsprocedures. Het Microsoft-beveiligingsbeleid bevat regels en vereisten waaraan moet worden voldaan bij de levering en werking van M365. Meer gedetailleerde vereisten zijn vastgelegd in de beveiligingsprocedures van M365 en de Standard Operating Procedures (SOP's) van het M365-team. Deze standaarden en procedures fungeren als aanvullingen op het Microsoft-beveiligingsbeleid en bieden details op implementatieniveau om specifieke operationele taken uit te voeren. Als zodanig controleren M365-teams regelmatig of ze voldoen aan het juiste beveiligingsbeleid, de juiste normen en andere beveiligingsnormen. Er worden passende maatregelen genomen als naar aanleiding van de beoordeling een niet-naleving wordt geconstateerd. Uit bovenstaande is op te maken dat de naleving van beveiligingsbeleid en -normen wordt beoordeeld.		
18.2.2.1	In de P&C-cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording.	CA-02 CA-07 CA-10 CA-53 ELC-04	SOC2 - 19 SOC2 - 20 ELC - 2 ELC - 5	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	

		Normen in assurance rapportages		Uitkomst onderzoeken werkgroep		Aandachtspunten gebruikersorganisatie
	BIO control/Overheidsmaatregel	M365	Azure	M365	Azure	CUEC
18.2.3	Beoordeling van technische naleving: Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	CA-27 CA-38 CA-45 CA-46 CA-48	VM - 6 VM - 8 CM - 8	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	M365 - CUEC-06: De gebruikersorganisaties is verantwoordelijk voor het beveiligen van de software en hardware die worden gebruikt om toegang te krijgen tot M365.
18.2.3.1	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.	CA-27 CA-38 CA-45 CA-46 CA-48	VM - 6 VM - 8 CM - 8	Controls aanwezig in assurance rapportage (SOC)	Controls aanwezig in assurance rapportage (SOC)	Zie 18.2.3

1 Bijlage - Reactie Microsoft

In deze bijlage is de reactie opgenomen vanuit Microsoft Corporation (MSFT). De door MSFT gegeven reactie heeft enkel betrekking op de controls die niet als zodanig zijn beschreven in de verkregen assurance rapportages of certificeringen.

BIO #	BC/OM	Omschrijving	M365	Azure	Geen controls beschreven	MSFT Response
9.4.4.2	OM	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	X	X	Het gebruik van systeemhulpmiddelen wordt niet expliciet opgenomen in de assurance- rapportages en/of controls. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Hieruit is niet duidelijk op te maken of het gebruik van deze systeemhulpmiddelen gelogd wordt, en hoe lang deze logging beschikbaar is voor onderzoek.	Toegang tot systemen binnen M365 vereist expliciete autorisatie, dit omvat ook de volgende beveiligingsgerelateerde functies: het instellen van systeemaccounts, het configureren van toegangsautorisaties (d.w.z. machtigingen, privileges), het instellen van te controleren gebeurtenissen en systeem- en beveiligingsbeheer. Deze functies omvatten ook het gebruik van hulpprogramma's. De autorisatiesystemen worden volledig gelogd en gemonitord en de logbestanden worden minimaal een jaar bijgehouden. De volgende controls, geaudit onder FedRAMP en vermeld in de FedRAMP SSP-documentatie welke Microsoft publiekelijk beschikbaar stelt, bieden een beschrijving van hoe Microsoft omgaat met de vereisten onder deze BIO-control: MA-04: "*M365 personnel do not have local access to production equipment. The use of non-local maintenance and diagnostic tools is a business requirement for the system. All M365 access and non-local maintenance is performed through the remote access points as documented in AC-17"* AC-6 (1): *"Service teams employ the concept of least privilege, allowing only pre-authorized accesses for service team administrators (and processes acting on behalf of service team administrators) which are necessary to accomplish assigned tasks in accordance with business functions and organizational need. Service owners employ the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to operational assets, individuals, and/or other organizations.*

BIO #	BC/OM	Omschrijving	M365	Azure	Geen controls beschreven	MSFT Response
						All access to the M365 system must be explicitly authorized, including the following security related functions: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and system and security administration. Role owners are responsible for reviewing and approving role assignments, and roles are tailored for different job functions such that personnel only have the minimum access required to perform their duties. For some teams, service team accounts by default belong to a security group that only has user-level operating system access to the production environment for that service team--this does not permit access to customer content. Access to any higher level of permissions must be requested through JIT tools and authorized by the on-call approver. Through the use of this just in time model, M365 explicitly authorizes access to security functions. AC-6 (9): *"All commands run by all accounts are logged."* AC-17: *"All remote access connections from service team personnel are audited utilizing the access points auditing functionality. The service team monitors the connections for attempted unauthorized use of M365 using Near Real Time Alerting tools. Two-factor authentication using YubiKeys through TSGs is the only approved method to gain remote administrative access to systems in any M365 domains.* *Logs from remote access points and customer-facing interfaces are uploaded to a repository service and reports are generated from those logs, in conjunction with the NRT Security Monitoring of remote access methods.* AU-11: "*M365 retains audit records in a repository service for at least one year to support investigations of security incidents and to meet regulatory retention requirements. Customers are allowed to copy and store their own audit records to meet customer storage requirements.*"
11.2.9.5	OM	Bij het gebruik van een chipcardtoken voor toegang	X	X	Uit assurance rapportages van Azure en M365 is niet op te	Een 'clean Desk'-beleid wordt voornamelijk geïmplementeerd door het afdwingen van mechanismen voor remote access.

BIO #	BC/OM	Omschrijving	M365	Azure	Geen controls beschreven	MSFT Response
		tot systemen wordt bij het verwijderen van de token de toegangsbeveiligingslock automatisch geactiveerd.			maken of gebruik wordt gemaakt van chipcardtokens. Daarnaast in M365 assurance rapportage geen control voor een policy voor clear-desk en clear-screen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Hieruit is niet op te maken of de beveiligingslock wordt geactiveerd bij het verwijderen van de token (smartcard).	Microsoft gebruikt YubiKey-tokens als multifactor-authenticatiemiddel om de toegang tot productiesystemen te controleren en te beschermen. De Yubikey-tokens vereisen na elke 5 minuten een capacitieve aanraking, waardoor de fysieke aanwezigheid van de gebruiker wordt geverifieerd. Dit is een effectieve bescherming tegen het risico dat smartcards achterblijven op specifieke (beheer)apparaten zoals de Secure Access Workstations (SAW's) die Microsoft gebruikt. Bovendien heeft Microsoft een vergrendelingsbeleid voor beheerapparaten en externe toegangsstations voor maximaal 15 minuten inactiviteit. De volgende controls, geaudit onder FedRAMP en vermeld in de FedRAMP SSP-documentatie die Microsoft publiekelijk beschikbaar stelt, bieden een beschrijving van hoe Microsoft omgaat met de vereisten onder deze BIO-control: AC-20(1): "*M365 only allows remote connections via secure remote desktops known as Secure Access Workstations (SAWs). These remote desktop sessions are locked down to only allow very limited and specific access. This access does not allow broad network access into production by the remote machines. The network access is limited to one specific protocol, and traffic is only allowed to specific bastion machines.* *Additionally, M365 has implemented compensating controls outlined below:* *• Minimal amount of data can be copied. There is a buffer limit on the clipboard.* *• M365 requires Two-Factor Authentication (2FA).* *• The M365 Security Incident Response capability is improved through unifying the available remote access methods.* *• M365 requires Just-In-Time (JIT) access, limiting access into production.*

BIO #	BC/OM	Omschrijving	M365	Azure	Geen controls beschreven	MSFT Response
						• External devices are logically prevented from connecting to the production environment. *• Aggressive idle time-outs are in place.* *• All M365 administrators are required to take security training.* *• No customer content is processed, stored, or transmitted.* *• All connections are encrypted via TLS 1.2 or higher."* MA-4: "*All M365 access and non-local maintenance is performed through the remote access points as documented in AC-17. Connection to the remote access point requires use of IAL, AAL, FAL level 3 and FIPS 140-2 compliant YubiKeys or approved IAL, AAL, FAL level 3 and FIPS 140-2 compliant TPM modules as described in IA-02(1). Connection from the remote access point to a particular server requires strong authentication as described in IA-05. All access to M365 is authorized, controlled, and approved as defined in AC-02."* AC-17.1: "*All remote access connections from service team personnel are audited utilizing the access points auditing functionality. The service team monitors the connections for attempted unauthorized use of M365 using Near Real Time Alerting tools. Two-factor authentication using YubiKeys through TSGs is the only approved method to gain remote administrative access to systems in any M365 domains."* AC -12: "*Additionally, service team administrator sessions are disconnected after no more than 15 minutes of inactivity.* AC-11: "*All M365 servers and Terminal Services Gateways managed by TSG or Azure run Windows. Compliance with this control is a built-in feature of Microsoft Windows. Microsoft Windows places a publicly-viewable pattern onto the associated display when the session lock mechanism is activated on a device with a display screen, hiding what was previously visible on the screen*"
12.4.2.3	OM	Er is een (onafhankelijke) interne audit procedure die	X	X	Interne audit procedure die minimaal halfjaarlijks toetst op het	Microsoft beschermt tegen het wijzigen, verwijderen of aanpassen van systeem gegenereerde logbestanden en bewaart beveiligingslogs ten

BIO #	BC/OM	Omschrijving	M365	Azure	Geen controls beschreven	MSFT Response
		minimaal halfjaarlijks toetst op het ongewijzigd bestaan van logbestanden.			ongewijzigd bestaan van logbestanden staat niet beschreven in M365 en Azure rapportage of aanvullende stukken.	minste één jaar ter ondersteuning van onderzoeken naar beveiligingsincidenten en om te voldoen aan wettelijke bewaarvereisten. Deze maatregelen en controls worden onafhankelijk geverifieerd via verschillende audits (audits van derden), waarbij FedRAMP voortdurende monitoring vereist. De volgende controls, geaudit onder FedRAMP en vermeld in de FedRAMP SSP-documentatie die Microsoft publiekelijk beschikbaar stelt, bieden een beschrijving van hoe Microsoft omgaat met de vereisten onder deze BIO-control: AU -9: "*Only M365 service team administrators have access to security logs. If a service team administrator deletes log data locally, this activity is logged, and an alert is generated. Audit information (…) is hashed and/or encrypted and can only be read when accessed through M365 by an authorized user. Authorized M365 personnel are only able to read information stored in the repository service and are not granted permissions to modify or delete logs."* AU-9 (2): *"Each M365 server uploads audit logs to a centralized repository service. In the event that real-time log shipping fails, logs are retained on the server until the connection is reinstated and they can be exported to the repository service."* AU-9(4): "*M365 restricts management of audit functionality within M365 to a limited subset of Service Engineer Operations personnel responsible for audit functionality. These personnel do not have the ability to modify or delete audit records that are stored in a repository service, and if they disable logging to the repository service, that action itself is logged. Repository service personnel do not have access to M365 MT."* AU-11: "*M365 retains audit records in a repository service for at least one year to support investigations of security incidents and to meet*

BIO #	BC/OM	Omschrijving	M365	Azure	Geen controls beschreven	MSFT Response
						regulatory retention requirements. Customers are allowed to copy and store their own audit records to meet customer storage requirements."
15.1.2.2	OM	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.	X	X	Uit assurance rapportages van Azure en M365 niet op te maken of prestatie-indicatoren en verantwoordingsrapportages worden opgenomen in inkoopcontracten. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Uit bovenstaande is niet op te maken of in de inkoopcontracten expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages worden opgenomen.	Onderdeel van het Microsoft Supplier Program (MSP) is dat alle subverwerkers en onderaannemers verplicht zijn om via het Microsoft Supplier Security and Privacy Assurance (MSSPA - https://www.microsoft.com/en-us/procurement/sspa) programma de veiligheid en vertrouwelijkheid van klant- en persoonsgegevens te waarborgen. Subverwerkers zijn contractueel verplicht om te voldoen aan strikte privacy- en beveiligingsvereisten die gelijkwaardig zijn aan of sterker zijn dan de contractuele verplichtingen die Microsoft aan zijn klanten maakt in het Online Services Data Protection Addendum. Subverwerkers ondertekenen ook de modelcontracten (Standard Contractual Clauses (SCC's)) en zijn verplicht om te voldoen aan de AVG-vereisten, inclusief de vereisten met betrekking tot het implementeren van passende technische en organisatorische maatregelen om persoonsgegevens te beschermen. Leveranciers kunnen zichzelf niet aanmerken als subverwerker bij Microsoft, omdat hiervoor goedkeuring vereist is door interne privacyteams van Microsoft. Leveranciers kunnen alleen een subverwerker zijn als Microsoft de verwerker is en de leverancier de daarvoor in aanmerking komende data categorieën verwerkt. Deze subverwerkers worden ingezet onder aanvullende contract- en nalevingsvereisten. Deze aanvullende contractvereisten zijn de SCC's en de Microsoft Online Services Customer Data Protection Addendum (OCDA). De OCDA bevat naast algemene gegevensbeschermingsvereisten (Data Protection Requirements (DPR)) vanuit het Microsoft Supplier Security and Privacy Assurance programma (MSSPA), ook additionele contractuele toezeggingen die tegemoet komen aan de vereisten uit de DPA welke: "*ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by the*

BIO #	BC/OM	Omschrijving	M365	Azure	Geen controls beschreven	MSFT Response
						DPA, including the limitations on disclosure of Processed Data. Microsoft agrees to oversee the Subprocessors to ensure that these contractual obligations are met". De contractuele security en privacy-vereisten worden jaarlijks onafhankelijk getoetst via het SSPA-programma. De zogenaamde Supplier Data Protection Requirements kunnen worden gebruikt door onafhankelijke auditors om deze supplier assurance evaluaties uit te voeren. In algemene zin biedt het Microsoft Supplier Program inzicht in de specifieke contractuele vereisten voor de gegevensbeschermings en beveiliging die Microsoft aan leveranciers stelt. Hieronder zijn verwijzingen opgenomen naar FedRAMP-controls en de openbaar beschikbare contractuele documentatie over het Microsoft Supplier Program (https://www.microsoft.com/en-us/procurement). De volgende controls, geaudit onder FedRAMP en vermeld in de FedRAMP SSP-documentatie die Microsoft publiekelijk beschikbaar stelt, bieden een beschrijving van hoe Microsoft omgaat met de vereisten onder deze BIO-control: SA-9: "*Microsoft requires all third parties (external information system services) who are engaged with M365 to sign a Master Supplier Services Agreement (MSSA). The MSSA requires the third party to comply with all applicable Microsoft security policies and implement security procedures to prevent disclosure of Microsoft confidential information. Microsoft includes provisions in the MSSA and any associated Statements of Work (SOW) with each vendor addressing the need to employ appropriate security controls. Vendors that handle sensitive data must be in compliance with Microsoft vendor privacy practices and data protection requirements.* SA-4: "*arrangements must be made in a formal contract to define responsibility and requirements for the security, confidentiality, integrity and availability of the information assets involved*." SA-12: *"M365 follows Microsoft system development life cycle which includes specific security considerations and critical security review and*

BIO #	BC/OM	Omschrijving	M365	Azure	Geen controls beschreven	MSFT Response
						approval checkpoints. The "M365 Information Security Policy" outlines software usage restrictions for M365, and require all applications, including those developed or hosted by and/or purchased from third parties, to undergo a comprehensive security review before entry into Microsoft Online environments. In addition, any new or changed resources may not be deployed or utilized in M365 without formal approval as required by M365 change management processes. M365's implementation of acquisitions control is described in SA-4. Prior to procurement, vendors must meet the requirements to participate in the Microsoft Supplier Program (MSP). All suppliers and purchase orders are vetted through Microsoft's procurement processes. The purchasing and allocation of all hardware components is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). The Microsoft Cloud Supply Chain (MCSC) group consists of six unique teams (Procurement, Customer Operations, Deployment Quality, Supplier Relationship Management, and Spares), each contributing to protecting Azure from threats to the Supply Chain." De volgende referenties bieden assurance vanuit het Microsoft Supplier Program: Vereisten voor leveranciers in the SSPA Program guide: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE47KhH Vereisten voor gegevensbescherming in de DPR, met daarin voor elke KPI en vereiste een expliciete verwijzingen naar "*Evidence of Compliance*": https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4gQoY
15.1.2.5	OM	Voordat een contract wordt afgesloten, wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete	X	X	Uit assurance rapportages van Azure en M365 niet op te maken dat de risicoafweging betrekking heeft op de afhankelijkheid. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-	Zie het antwoord op 15.1.2.2 voor meer informatie over de contractering onder het Microsoft Supplier Program. Contractueel zijn er verschillende specifieke clausules opgenomen met betrekking tot beëindiging en exit. Zie: · MSSA (Master Supplier Services Agreement), Section 5, Term and Termination · DPR (Data Protection Requirements), Section E:13

BIO #	BC/OM	Omschrijving	M365	Azure	Geen controls beschreven	MSFT Response
		uitwerking van de exit-strategie.			certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Uit bovenstaande is voor M365 en Azure niet op te maken dat een expliciete uitwerking van de exit-strategie een vast onderdeel van het contract is.	Document hier is beschikbaar: https://www.microsoft.com/en-us/procurement/ssp
15.1.3.1	OM	Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.	X	X	Uit assurance rapportages van Azure en M365 niet op te maken of leveranciers hun toeleveranciers bekend moeten maken en eisen hieraan op leggen. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Uit bovenstaande is niet op te maken dat leveranciers hun keten van toeleveranciers bekend moeten maken en transparant moeten zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.	Zie het antwoord op 15.1.2.2 voor meer informatie over de contractering onder het Microsoft Supplier Program. Contractueel zijn er verschillende specifieke clausules opgenomen met betrekking tot subprocessors en Microsoft-leveranciers. Zie: · SSPA guide, Section “Use of Subcontractors” · MSSA (Master Supplier Services Agreement), Section 2 (i) – Supplier’s personnel and subcontracting · DPR (Data Protection Requirements), Section G: Subcontractors Document hier beschikbaar: https://www.microsoft.com/en-us/procurement/ssp
15.2.1.1	OM	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging	X	X	Uit assurance rapportages van Azure en M365 niet op te maken of de prestatie jaarlijks wordt beoordeeld op dezelfde	Zie het antwoord op 15.1.2.2 voor meer informatie over de contractering onder het Microsoft Supplier Program. Zie specifiek de vereisten in de SSPA-guide: *“if the supplier has a Data Processing Role of “Subprocessor”, the supplier cannot change this*

BIO #	BC/OM	Omschrijving	M365	Azure	Geen controls beschreven	MSFT Response
		beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.			indicatoren als opgenomen in contracten. Hiervoor is aanvullende informatie aangeleverd door Microsoft. Dit betreft rapportages (geen assurance) over ISO27001-certificering (2016) voor M365 en het NIST-framework (2021) voor Azure. Uit bovenstaande is niet op te maken dat de prestatie van leveranciers op het gebied van informatiebeveiliging jaarlijks wordt beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.	*approval and will be required to have an Independent Assessment conducted annually.* Leveranciers kunnen zichzelf niet aanmerken als subverwerker bij Microsoft, omdat hiervoor goedkeuring vereist is door interne privacyteams van Microsoft. Leveranciers kunnen alleen een subverwerker zijn als Microsoft de verwerker is en de leverancier de daarvoor in aanmerking komende data categorieën verwerkt. Deze subverwerkers worden ingezet onder aanvullende contract- en nalevingsvereisten.
16.1.2.7	OM	Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD) procedure is onderdeel van de incidentrapportage.		X	Het is niet mogelijk om uit assurance- rapportages op te maken of informatie uit de CVD-procedure onderdeel is van de incidentrapportage. Ook voor Azure is online op te maken dat een bug bounty programma opgezet (https://www.microsoft.com/en-us/msrc/bounty-microsoft-azure). Hieruit is niet op te maken of de informatie afkomstig uit de CVD-procedure onderdeel is van de incident rapportage.	Microsoft maakt gebruik van de CVD-procedure dat onderdeel is van het Microsoft Security Response Center (MSRC). Zie: https://msrc.microsoft.com/create-report?c=faq en https://www.microsoft.com/en-us/msrc/faqs-report-an-issue waar de CVD te vinden is. Informatie uit de MSRC wordt binnen Microsoft 365 en Azure gebruikt als onderdeel van kwetsbaarheidsbeheer en incidentbeheerrapportage. De volgende controls, geaudit onder FedRAMP en vermeld in de FedRAMP SSP-documentatie die Microsoft publiekelijk beschikbaar stelt, bieden een beschrijving van hoe Microsoft omgaat met de vereisten onder deze BIO-control: CA-7(1): geeft aan hoe information van het MSRC gebruikt wordt binnen M3655 incident rapportages: ‘’*M365 receives information system security alerts, advisories, and directives from a number of external communications including US-CERT, Customer incident*

BIO #	BC/OM	Omschrijving	M365	Azure	Geen controls beschreven	MSFT Response
						reports, Microsoft OSSC C+AI Security Operations Center (SOC) and MSRC. Trend analysis is used to determine if changes need to be made to the overall continuous monitoring strategy." IR-4: "*The M365 Security Incident Response Plan identifies information appropriate to correlate and share with US-CERT and incident handling teams for affected customers to achieve a wider perspective on incident awareness. M365 coordinates with these other organizations to correlate and share this information.* *The Azure C+AI Security Operations Center (SOC) team coordinates and leverages various sources for incident awareness such as US-Cert/DoD Cert, MSRC, Adobe, CISCO, CVE, and Qualys. The C+AI Security Operations Center (SOC) team utilizes a Microsoft incident reporting website (http://cert.microsoft.com) that is based on the US CERT Incident Reporting System (https://forms.us-cert.gov/report/).* *For effective incident responses, the C+AI Operations Center (SOC) Team coordinates with major applications and the Threat Intelligence committee in order to collaborate and share relevant and critical incident handling information that have a cross organization impact.* SI-2: "*M365 identifies, reports, and corrects information system flaws through vulnerability management, incident response management, and patch/configuration management processes. The M365 Security Incident Response Program assists with identifying and reporting of information system flaws. M365 receives vulnerability-related data from multiple sources of information which include: Microsoft Security Resource Center (MSRC), vendor Websites, other third-party services (e.g. Internet Security Systems) and internal/external vulnerability scanning of services.* RA-5: "*M365 Security also provides a reporting interface to allow authorized M365 personnel to see the details of vulnerabilities*

BIO #	BC/OM	Omschrijving	M365	Azure	Geen controls beschreven	MSFT Response
						associated with the environment. The reporting interface provides high-level / technical reports (covering information such as servers, vulnerabilities, CVE IDs, breakdowns of vulnerable hosts, and remediation steps). The M365 service teams utilize the information on the reporting interface to ensure that servers are compliant with M365 vulnerability management standards".