KPMG

Microsoft Office 365 and Azure

BIR coverage

Report for Microsoft B.V.

KPMG Advisory N.V.

4 November 2016 (v.1.00)

A1500006694

Contents

KPMG contacts:

Koos Wolters RE CISA
Partner
+31 20 656 4048
wolters.koos@kpmg.nl

Edwin Sturrus MSc CCSK
Senior Consultant
+31 20 656 7248
sturrus.edwin@kpmg.nl

Olga Kulikova MSc CCSK
Senior Consultant
+31 20 656 8776
kulikova.olga@kpmg.nl

Executive Summary

Organizations operating in the government sector have to demonstrate compliance with the Baseline Informatiebeveiliging Rijksdienst standard (hereafter: BIR). In order to do so, these organizations have to perform periodic audits against this standard. When using Microsoft Office 365 and/or Azure, part of the BIR controls for these specific solutions are managed by Microsoft. Organizations that need to comply with BIR are therefore obliged to also determine if the Microsoft services they are using are compliant with this standard.

Microsoft Office 365 and Azure undergo various periodic independent certifications and assurance statements, some of which closely related to BIR. On request of Microsoft B.V. (hereafter: Microsoft), we analyzed the extent to which current certifications and assurance statements cover the part of BIR that Microsoft is responsible for with Office 365 and Azure.

Based on our analysis we determined that:

- For **Microsoft Office 365**, 91% of the BIR controls are either covered by certifications or assurance standards or are not in scope, 9% (37 out of 399) controls are currently not covered. Microsoft has provided a detailed response in this report with suggestions on how compliance with these controls could be demonstrated.
- For **Microsoft Azure**, 92% of the BIR controls are covered by certifications or assurance standards, 8% (33 out of 399) of the controls are currently not covered. Microsoft has provided a detailed response in this report with suggestions on how compliance with these controls could be demonstrated.

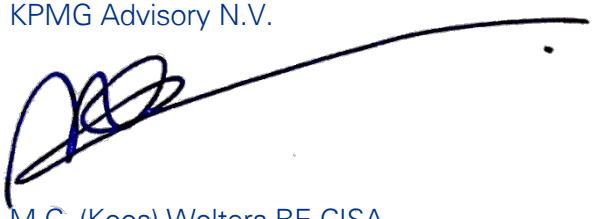
Our analysis only focused on (parts of) the controls that are relevant for the Microsoft products Office 365 and Azure, and for which Microsoft is responsible. It indicates to what extent the use of Office 365 or Azure will (not) limit organizations to demonstrate compliance with BIR.

In addition, organizations using Office 365 and/or Azure that need to comply with BIR, need to address the following topics themselves: identity & access management, data classification, data backup, retention and removal, data leakage prevention, encryption & key management, data integrity and log data protection. For more details please refer to the next sections in this report.

It was a pleasure working with Microsoft on this engagement. Should you have any questions about any aspect of this report, feel free to contact Mr. Edwin Sturrus, Ms. Olga Kulikova or undersigned. Please refer to page 2 for contact details.

Yours sincerely,

KPMG Advisory N.V.



M.C. (Koos) Wolters RE CISA

Partner

Introduction and objective

Introduction

There is a growing demand for cloud services. This is a development we see worldwide as well as in the Netherlands. Microsoft sees this growth reflected in the demand for its Azure and Office 365 offerings, across a wide variety of customers and sectors. Among these are customers in the government sector. These organizations often process classified and privacy sensitive information. In order to demonstrate control over security and privacy of this data, government organizations have to comply with the BIR standard.

Microsoft is not subject to compliance with BIR. However, customers from the government sector are seeking ways to demonstrate compliance with BIR, when using cloud services such as Azure or Office 365.

Microsoft's cloud services undergo various periodic certifications and assurance statements, some of these are closely related to BIR. We analyzed to what extent current certifications and assurance statements cover the parts of the BIR controls that relate to Microsoft as a cloud service provider.

For more details regarding the BIR standard, please refer to Appendix B.

Objective

The objective of this analysis is to provide insight in the coverage of the part of BIR for which Microsoft is responsible, by certifications and assurance statements of Microsoft Office 365 and Microsoft Azure. Microsoft is responsible for these parts of controls that relate directly to the Office 365 or Azure service offerings. In order to comply with BIR, the remaining parts have to be covered by the organization using Office 365 and/or Azure.

Organizations subject to compliance with the BIR standard, can use these results to determine their compliance with this standard, when using Office 365 and/or Azure.

Scope and approach

Scope

The scope of our analysis of Office 365 and Azure is limited to the BIR standard and the extent to which this standard is covered by assurance statements and certifications. Our analysis covers standard offerings and does not consider additional security technologies, that are under the control of the customer to configure and use. Other services provided by Microsoft, which are connected to Office 365 and/or Azure, may be mentioned where relevant to BIR, but were not the subject of our analysis.

BIR consists of 133 subcategories, based on ISO 27001:2005. There are 266 specific additions for government organizations divided over the subcategories. This makes a total of 399 controls.

Of the 266 specific additions, only 92 are described as applicable controls (R-controls), when there is an ISO 27001 certification. Therefore, we focused our research on the 225 (133 + 92) relevant controls. The remaining 174 (266 -/- 92) specific additions are designated as out of scope.

Our analysis focused specifically on the SOC 2 and ISO 27001:2013 certifications for Office 365, Azure and, where relevant, the underlying Microsoft Cloud Infrastructure and Operations (MCIO). For details on the applicability of certifications to these products, please refer to the 'Microsoft Compliance Framework for Industry Standards and Regulations'.

Approach

As part of our analysis:

- we designed mappings from BIR to the ISO 27001:2013 certification and SOC 2 assurance statements;
- we analyzed the statement of applicability of ISO 27001:2013 and the detailed SOC 2 results, to determine to what extent these cover the BIR controls;
- we analyzed the ISO 27001:2013 and SOC 2 for MCIO, for the BIR controls that rely on infrastructure components;
- we analyzed the OST for specific contractual statements and FedRAMP for additional technical details related to the BIR controls;
- we defined customer considerations when using Office 365 or Azure.

Limitations

Limitations

This report does not intend to provide any assurance in itself or to replace any assurance or certification.

The information contained in this report is private and confidential. This report has been prepared solely for the purpose stated herein and should not be used for any other purpose. Except as specifically stated in the report, neither our report nor its contents are to be referred to or quoted externally, in whole or in part, without our prior written approval. In addition, except as set forth in the report, our analysis and report are not intended for general circulation or publication, nor are they to be reproduced or distributed to any third parties without our prior written consent.

This report is provided on the basis that it is for your information only and that it will not be copied or disclosed via other channels than the Microsoft Service Trust Portal.

Our findings in this document are limited to the information specifically set forth herein and are based on the completeness and accuracy of the information provided to us by Microsoft. We have not audited or otherwise verified the accuracy or completeness of the records or other information given to us.

If any of the foregoing facts, assumptions or representations is not entirely complete or accurate, it is imperative that we be informed immediately, as the inaccuracy or incompleteness could have a material effect on the contents of this report.

We will not update our findings for subsequent changes or modifications to the law and regulations or to the judicial and administrative interpretations thereof.

We are not expressing any assurance with respect to the security of Microsoft's IT environment, infrastructure or services. Our report does not assess specific service and systems functionality, calculation algorithms and/or results from data processing. We are not responsible for the complete compliance of the information systems deployed at the organization with internal regulations. We are not responsible for establishing all risks and errors in the reviewed systems and in the interfaces with the other systems.

The management response sections of this report have been included based on the representations of Microsoft in July 2016. We have not verified the accuracy or veracity of the statements made, and do not provide any warranty of the accuracy of the response.

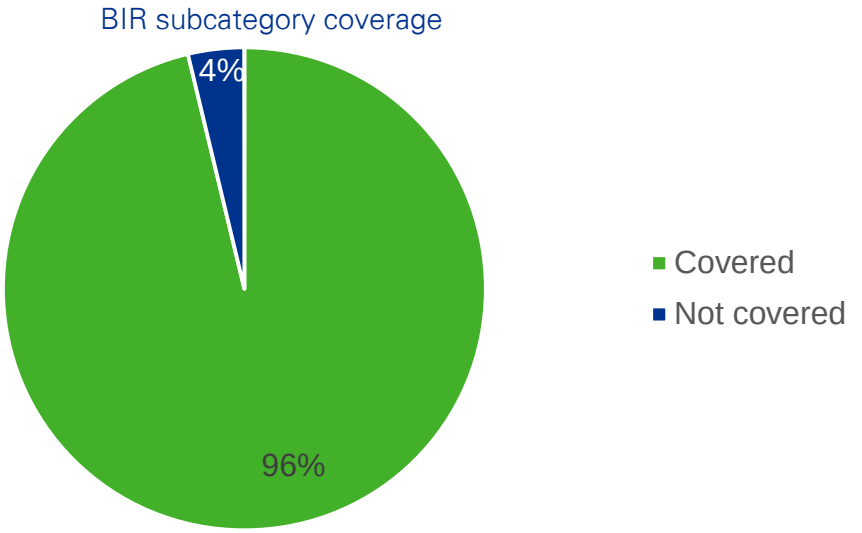
Results (Office 365)

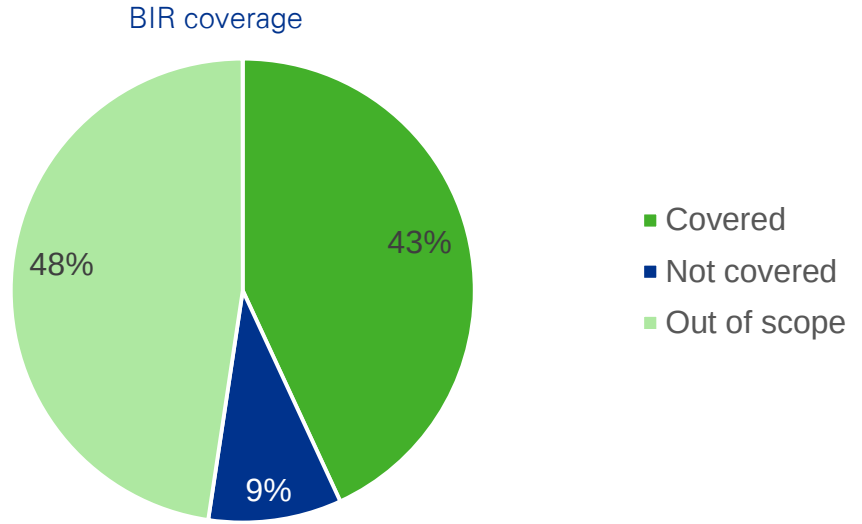
In total, 128 of the 133 subcategories in BIR are covered by ISO 27001:2013, SOC 2, FedRAMP, OST or a combination of those; 5 of these 133 subcategories are not covered, due to differences between ISO 27001:2005, on which BIR is based, and ISO 27001:2013.

In total, 362 of the 399 controls in BIR are either covered by ISO 27001:2013, SOC 2, FedRAMP, OST or a combination of those, or are out of scope; 37 of these 399 controls are not covered.

For the controls that are not covered, Microsoft has provided a detailed response with suggestions on how compliance with these controls could be demonstrated.

For more details regarding the numbers refer to the tables on the next page, the graphs on the right, and Appendix A.





Results (Office 365) (cont.)

BIR subcategory coverage

Result	#	%
Total	133	100
Out of scope	0	0
Covered	128	96
Not covered	5	4

BIR coverage

Result	#	%
Total	399	100
Out of scope	190	48
Specific additions not in scope	*174*	*44*
No responsibility Microsoft	*16*	*4*
Covered	172	43
ISO 27001:2013 and SOC 2	*98*	*25*
ISO27001:2013, SOC 2 and FedRAMP	*3*	*1*
ISO 27001:2013 only	*30*	*8*
SOC 2 only	*8*	*2*
SOC 2 and FedRAMP	*4*	*1*
FedRAMP only	*25*	*5*
OST only	*4*	*1*
Not covered	37	9

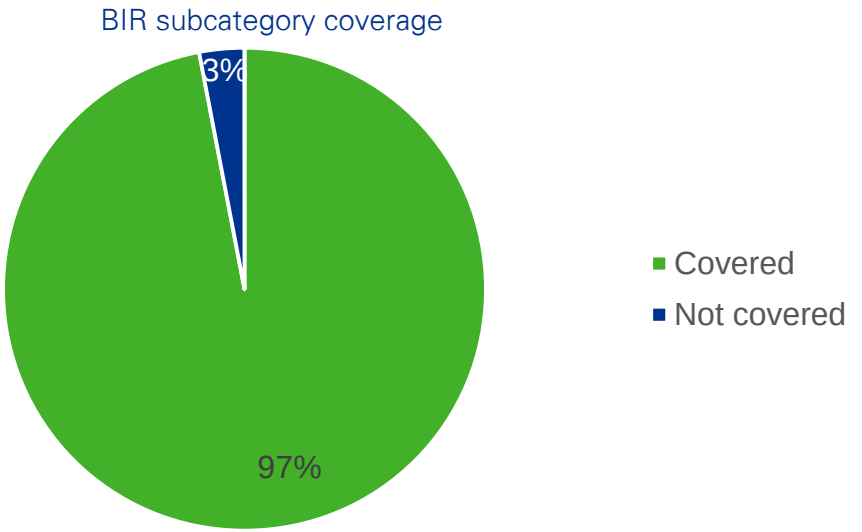
Results (Azure)

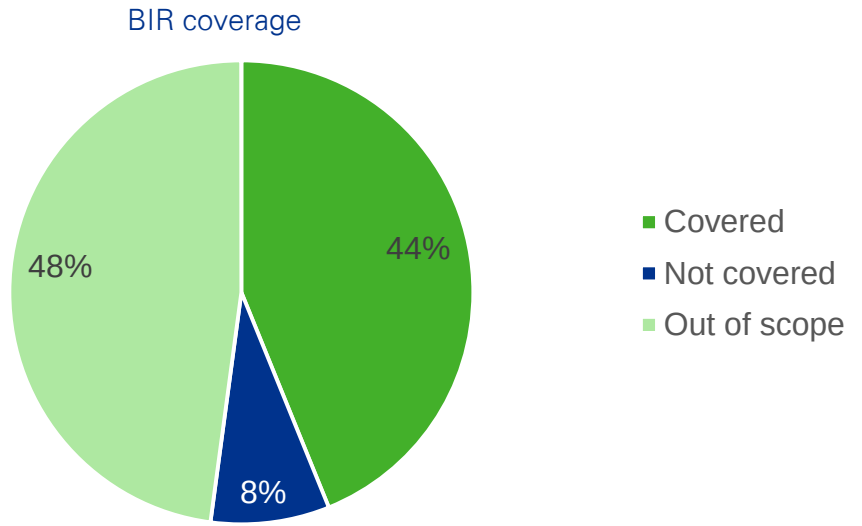
In total, 129 of the 133 subcategories in BIR are covered by ISO 27001:2013, SOC 2, FedRAMP, OST or a combination of those; 4 of these 133 subcategories are not covered, due to differences between ISO 27001:2005, on which BIR is based, and ISO 27001:2013.

In total, 366 of the 399 controls in BIR are either covered by ISO 27001:2013, SOC 2, FedRAMP, OST or a combination of those, or are out of scope; 33 of these 399 controls are not covered.

For the controls that are not covered, Microsoft has provided a detailed response with suggestions on how compliance with these controls could be demonstrated.

For more details regarding the numbers refer to the tables on the next page, the graphs on the right, and Appendix A.





Results (Azure) (cont.)

BIR subcategory coverage

Result	#	%
Total	133	100
Out of scope	0	0
Covered	129	97
Not covered	4	3

BIR coverage

Result	#	%
Total	399	100
Out of scope	191	48
Specific additions not in scope	*174*	*44*
No responsibility Microsoft	*17*	*4*
Covered	175	44
ISO 27001:2013 and SOC 2	*98*	*25*
ISO27001:2013, SOC 2 and FedRAMP	*3*	*1*
ISO 27001:2013 only	*30*	*8*
SOC 2 only	*8*	*2*
SOC 2 and FedRAMP	*4*	*1*
FedRAMP only	*28*	*6*
OST only	*4*	*1*
Not covered	33	8

Key customer considerations

Demonstrating compliance with the BIR standard is the responsibility of the organization using the cloud service. The results above indicate to what extent current certifications, assurance statements and contracts for Office 365 and Azure cover the applicable parts of the BIR controls for which Microsoft is responsible. This coverage can help organizations understand to what extent the ability to demonstrate compliance with BIR may be limited when using Office 365 or Azure.

Below we summarized the key considerations that government organizations should cover in order to be able to demonstrate compliance with BIR, when using Microsoft Office 365 or Azure. For more details regarding the key considerations, please refer to the detailed results in Appendix A.

Microsoft Office 365

Identity and access management

- Centrally manage users, authentication mechanisms and authorizations to and in Office 365.
- Configure data sharing privileges in Office 365, based on location, data type and domains.

Data management

- Ensure effective classification and labelling of data and apply access and sharing policies based on the specific types of data to prevent unauthorized access and sharing of sensitive information.
- Consider archiving data that has to be stored read-only for multiple years.
- Ensure backups are created outside of the solution for critical data.
- Perform data integrity checks when exporting data from and importing data to Office 365.

For more details regarding data resiliency in Office 365, please refer to the Microsoft 'Data Resiliency in Office 365' whitepaper.

Key customer considerations (cont.)

Microsoft Azure

Data backup and resilience

- Ensure that backups of data residing within applications are made, to prevent data loss.
- Implement disaster recovery and business continuity plans that address the inability to access or utilize Microsoft Azure.

Encryption and key management

- Determine encryption requirements of sensitive data and implement appropriate levels of encryption and key management.
- Securely store the certificates used to access cloud services.

Logging and monitoring

- Ensure protection of log data, by pulling logs to secure environments for long-term storage and by loading them in SIEM solutions for active monitoring.

Patching

- Ensure timely review and roll-out security and regular patches for applications.
- Establish a process to update parts of the environment that are not part of the auto-update cycle of Microsoft.

Networking

- Design and implement interconnectivity between Azure and on-premises resources.
- Consider network redundancy for critical applications and systems.

KPMG

Appendices

Appendix A - Details on results

The following table covers the detailed results of our analysis. The table reflects the mapping of Microsoft Azure and Office 365 certifications, assurance statements and contracts with the BIR standard.

Table legend

Column title	Description
BIR #	Reference to BIR control.
Control Description	BIR control description.
Control Mapping	Comment on degree of mapping of BIR control to ISO 27001:2013 and SOC 2 controls.
Office 365	Controls from MS Office 365 ISO 27001:2013 and SOC 2 certifications that correspond to the BIR controls.
Azure	Controls from Azure ISO 27001:2013 and SOC 2 certifications that correspond to the BIR controls.
Other documentation	Reference to other Microsoft documents (such as Microsoft Online Service Terms (OST), Online SLAs, etc.) in case ISO 27001:2013 and SOC 2 assurance do not fully cover BIR control.
Customer considerations	Microsoft has no influence on (parts of) certain controls. For these controls the organization using the cloud services has to address specific aspects, listed here.

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
5.1.1	Een document met informatiebeveiligingsbeleid behoort door de directie te worden goedgekeurd en gepubliceerd en kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.	Covered by ISO 27001:2013 and SOC 2	5.1.1	CC2.4, CC2.3	5.1.1	CC2.4, CC2.3		
5.1.2	Het informatiebeveiligings-beleid behoort met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.	Covered by ISO 27001:2013 and SOC 2	5.1.2	CC4.1	5.1.2	CC4.1		
5.1.2.1	Het informatiebeveiligings-beleid wordt minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld. Zie ook 6.1.8.1.	Covered by ISO 27001:2013 and SOC 2	5.1.2	CC4.1	5.1.2	CC4.1		
6.1.1	De directie behoort actief beveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.	Covered by ISO 27001:2013 and SOC 2	6.1.1	CC1.1, CC1.2	6.1.1	CC1.1, CC1.2	OST: Security – Organization of Information Security	
6.1.1.1	Het lijnmanagement waarborgt dat de informatiebeveiligings-doelstellingen worden vastgesteld, voldoen aan de kaders zoals gesteld in dit document en zijn	Covered by SOC 2 only	n/a	SOC 2 – Commit-ment to compet ence	n/a	SOC 2 – Commit-ment to compe-tence		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	geïntegreerd in de relevante processen. Dit gebeurt door één keer per jaar opzet, bestaan en werking van de IB-maatregelen te bespreken in het overleg van de departementsleiding en hiervan verslag te doen. Zie ook het 'in control'-statement zoals beschreven in het VIR:2007.							
6.1.2	Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit verschillende delen van de organisatie met relevante rollen en functies.	Covered by ISO 27001:2013 and SOC 2	6.1.1, 6.1.4	CC2.1	6.1.1, 6.1.4	CC2.1	OST: Security – Organization of Information Security	
6.1.2.1	De rollen van BVA, BVC en het lijnmanagement zijn beschreven in het Beveiligingsvoorschrift Rijksdienst 2005. FG staat in WBP.	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		This control is specifically aimed towards government agencies and the customer is responsible for fulfilling all requirements of the control.
6.1.3	Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd.	Covered by ISO 27001:2013 and SOC 2	6.1.1	CC1.2, C1.4	6.1.1	CC1.2, C1.4	OST: Security – Organization of Information Security	To fulfill the requirements for this control, the customer is responsible for the assignment of the roles and responsi-bilities within the organization.
6.1.3.1	Elke lijnmanager is verantwoordelijk voor de integrale beveiliging van zijn of haar dienstonderdeel.	Covered by ISO 27001:2013 and SOC 2	6.1.1	CC1.2, C1.4	6.1.1	CC1.2, C1.4	OST: Security – Organization of Information Security	To fulfill the requirements for this control, the customer is responsible for the

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
								assignment of the roles and responsibilities within the organization.
6.1.4	Er behoort een goedkeuringsproces voor nieuwe IT-voorzieningen te worden vastgesteld en geïmplementeerd.	Covered by ISO 27001:2013 and SOC 2	8.1.1, 8.1.2, 8.1.3, 9.2.6	CC5.1	8.1.1, 8.1.2, 8.1.3, 9.2.6	CC5.1		
6.1.5	Eisen voor vertrouwelijkheid of geheimhoudings-overeenkomst die een weerslag vormen van de behoefte van de organisatie aan bescherming van informatie, behoren te worden vastgesteld en regelmatig te worden beoordeeld.	Covered by ISO 27001:2013 and SOC 2	13.2.4	CC1.4, C1.4	13.2.4	CC1.4, C1.4	OST: Privacy, Human Resources Security	
6.1.5.1	De algemene geheim-houdingsplicht voor ambtenaren is geregeld in de Ambtenarenwet art. 125a, lid 3. Daarnaast dienen personen die te maken hebben met Bijzondere Informatie een geheimhoudingsverklaring te ondertekenen (zie VIRBI); daaronder valt ook de departementaal vertrouwelijke informatie. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		This control is specifically aimed towards government agencies and the customer is responsible for fulfilling all requirements of the control.

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
6.1.6	Er behoren geschikte contacten met relevante overheidsinstanties te worden onderhouden.	Covered by ISO 27001:2013 only	6.1.3	n/a	6.1.3	n/a		
6.1.6.1	Het lijnmanagement stelt vast in welke gevallen en door wie er contacten met autoriteiten (brandweer, toezichthouders, etc.) worden onderhouden.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
Detailed response of Microsoft regarding '6.1.6.1'		We view the reference to 'lijnmanagement' to indicate this control is intended for the customer of the services. Microsoft has an organized structured approach for incident management that includes outreach to relevant authorities where appropriate. *Our Microsoft Operations Centers (MOCs) are globally distributed and work around the clock in a "follow-the-sun" model to ensure our cloud services are persistently available. Each MOC is staffed with a team of incident management professionals and collectively they are responsible for monitoring service health, process automation, infrastructure operations, event and crisis management, and communications across the business. They are responsible for more than five hundred service components and monitor the servers and devices for the services we provide. Most critically, this is the team that identifies and resolves service incidents and outages when things go wrong.* *In an environment with so many services, not all incidents are the same. Over half of all incidents are handled through automation and 90 percent of all incidents are handled at first touch. The most severe issues are resolved by a highly trained and qualified crisis management team, working on technical resolution, escalations, and communications to the impacted business groups.* Source: http://download.microsoft.com/download/C/5/5/C55C7170-9AA0-4187-9A78-C5AE85C8161D/Cloud_Infrastructure_Operational_Excellence_and_Reliability_Strategy_Brief.pdf *[1] Microsoft Disclaimer*					
6.1.7	Er behoren geschikte contacten met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties te worden onderhouden.	Covered by ISO 27001:2013 only	6.1.4	n/a	6.1.4	n/a		
6.1.8	De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan	Covered by ISO 27001:2013 and SOC 2	18.2.1	CC1.1, CC4.1	18.2.1	CC1.1, CC4.1		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	(d.w.z. beheers-doelstellingen, beheers-maatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich significante wijzigingen voordoen in de implementatie van de beveiliging.							
6.1.8.1	Het informatiebeveiligings-beleid wordt minimaal één keer in de drie jaar geëvalueerd (door een onafhankelijke deskundige) en desgewenst bijgesteld. Zie ook 5.1.2.	Covered by ISO 27001:2013 and SOC 2	5.1.2	CC4.1	5.1.2	CC4.1		
6.1.8.2	Periodieke beveiligingsaudits worden uitgevoerd in opdracht van het lijnmanagement.	Covered by ISO 27001:2013 and SOC 2	5.1.2	CC4.1	5.1.2	CC4.1		
6.2.1	De risico's voor de informatie- en IT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend.	Covered by ISO 27001:2013 and SOC 2	15.1.1, 15.1.2	C1.5	15.1.1, 15.1.2	CC3.1, CC3.2		
6.2.1.3	Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke	Covered by OST only	n/a	n/a	n/a	n/a	OST: Use of Subcontractors; MOSC: A8.2.2	To fulfill the requirements for this control, the customer is responsible for the

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	waarde en gevoeligheid de informatie (bijv. risicoklasse van WBP of vertrouwelijk-heidklasse volgens VIRBI) heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligings-maatregelen nodig zijn.							classification of data before sharing with third parties.
6.2.1.5	Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkerovereenkomst (conform WBP artikel 14) afgesloten.	Covered by OST only	n/a	n/a	n/a	n/a	OST: Use of Subcontractors	To fulfill the requirements for this control, the customer is responsible for getting a data processing agreement in place.
6.2.2	Alle geïdentificeerde beveiligingseisen behoren te worden behandeld voordat klanten toegang wordt verleend tot de informatie of bedrijfsmiddelen van de organisatie.	Covered by ISO 27001:2013 and SOC 2	9.1.1	CC2.1, CC2.2, CC5.2	9.1.1	CC2.1, CC2.2, CC5.2		
6.2.3	In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of IT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan IT-voorzieningen waarbij sprake is van toegang, behoren alle relevante beveiligingseisen te zijn opgenomen.	Covered by ISO 27001:2013 and SOC 2	15.1.2	CC2.2, C1.4, C1.5	15.1.2	CC2.2, C1.4, C1.5	OST: Use of Subcontractors	
7.1.1	Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle	Covered by ISO 27001:2013 and SOC 2	8.1.1	CC7.2	8.1.1	CC7.2		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden.							
7.1.2	Alle informatie en bedrijfsmiddelen die verband houden met IT-voorzieningen behoren een eigenaar te hebben in de vorm van een aangewezen deel van de organisatie.	Covered by ISO 27001:2013 only	8.1.2	n/a	8.1.2	n/a	OST: Security – Asset Management	
7.1.3	Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie- en bedrijfs-middelen die verband houden met IT-voorzieningen.	Covered by ISO 27001:2013 only	8.1.3	n/a	8.1.3	n/a	OST: Security – Asset Management	
7.1.3.1	Er zijn regels voor acceptabel gebruik van bedrijfsmiddelen (met name internet, e-mail en mobiele apparatuur). Het ARAR verplicht ambtenaren zich hieraan te houden. Voor extern personeel is dit in het contract vastgelegd. Zie ook "Uitgangspunten online communicatie rijksambtenaren" (Ministerie van Algemene Zaken, 2010).	Covered by ISO 27001:2013 only	8.1.3	n/a	8.1.3	n/a	OST: Security-Asset Management	To fulfill the requirements for this control, the customer is responsible for ensuring compliancy with internal acceptable use policies.
7.1.3.4	Informatiedragers worden dusdanig gebruikt dat vertrouwelijke informatie niet beschikbaar kan komen voor onbevoegde personen.	Covered by ISO 27001:2013 and FedRAMP	8.2.2	n/a	8.2.2	n/a	OST: Security – Asset Management; MOSC: A8.2.2, A.10.5; FedRAMP: 13.10.3	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
7.2.1	Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.	Covered by ISO 27001:2013 only	8.2.1	n/a	8.2.1	n/a		
7.2.1.1	De organisatie heeft rubriceringsrichtlijnen opgesteld (ter invulling van het VIRBI).	Covered by ISO 27001:2013 only	8.2.1	n/a	8.2.1	n/a		To fulfill the requirements for this control, the customer is responsible for ensuring implementation of data classification.
7.2.2	Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd.	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		To fulfill the requirements for this control, the customer is responsible for ensuring that documents stored and processed by Microsoft Online Services are labeled and treated confidentially.
7.2.2.1	De lijnmanager heeft maatregelen (conform VIRBI) getroffen om te voorkomen dat niet-geautoriseerden kennis kunnen nemen van gerubriceerde informatie.	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		The customer is responsible for fulfilling the requirements for this control.
7.2.2.2	De opsteller van de informatie doet een voorstel tot rubricering en brengt deze aan op de informatie. De vaststeller van de inhoud van de informatie stelt tevens de rubricering vast.	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		The customer is responsible for fulfilling the requirements for this control.

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
8.1.1	De rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers ten aanzien van beveiliging behoren te worden vastgesteld en gedocumenteerd overeenkomstig het beleid voor informatiebeveiliging van de organisatie.	Covered by ISO 27001:2013 and SOC 2	6.1.1	CC1.1, CC1.2	6.1.1	CC1.1, CC1.2		
8.1.1.2	Alle ambtenaren en ingehuurde medewerkers krijgen bij hun aanstelling hun verantwoordelijkheden ten aanzien van informatie-beveiliging ter inzage. De schriftelijk vastgestelde en voor hen geldende regelingen en instructies ten aanzien van informatie-beveiliging, welke zij bij de vervulling van hun dienst hebben na te leven, worden op een gemakkelijk toegankelijke plaats ter inzage gelegd. Overeenkomstige voorschriften maken deel uit van de contracten met externe partijen. Ook voor hen geldt de toegankelijk-heid van geldende regelingen en instructies.	Covered by SOC 2 and OST	n/a	CC2.2	n/a	CC2.2	OST: Human Resource Training	
8.1.1.3	Indien een medewerker speciale verantwoordelijk-heden heeft t.a.v. informatie-beveiliging dan is hem dat voor indiensttreding (of bij functiewijziging), bij voorkeur	Covered by SOC 2 only	n/a	CC1.4	n/a	CC1.4	MOSC: A.7.1.2	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	in de aanstellingsbrief of bij het afsluiten van het contract, aantoonbaar duidelijk gemaakt.							
8.1.2	Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers, behoort te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en behoort evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.	Covered by ISO 27001:2013 and SOC 2	7.1.1	CC1.4	7.1.1	CC1.4		
8.1.2.1	Voor alle medewerkers (ambtenaren en externe medewerkers) is minimaal een relevante Verklaring Omtrent het Gedrag (VOG) vereist. Indien het een vertrouwensfunctie betreft wordt ook een veiligheids-onderzoek (Verklaring van Geen Bezwaar) uitgevoerd.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	CC1.4	n/a	CC1.4	FedRAMP: 13.13.3	
Detailed response of Microsoft regarding '8.1.2.1'		This control refers to regulatory frameworks that are specific to The Netherlands. The Microsoft Online Services are an international infrastructure, we ask the reader to interpret this control in the BIR from an 'or equivalent' perspective. The customer is responsible for implementing these requirements for their own personnel before they are granted access to the system. Microsoft screens personnel prior to providing access to customer data. The process for screening is available for review via a Microsoft representative. (Microsoft intranet document: https://microsoft.sharepoint.com/teams/Office 365sec/access/wiki/Pages/Clearance%20Requirements.aspx) Pursuant to local laws, regulations, ethics and contractual constraints, all Microsoft full-time employees (FTE) are required to successfully complete a standard background check as part of the hiring process. Background checks may include but are not limited to review of information relating to a candidate's education, employment, and criminal history.						

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
		In the event that a vendor will be working with government data, Microsoft ensures that vendor companies perform the necessary background investigations on their personnel and report their findings annually. Microsoft data center personnel do not work with customer data as they have no access to customer data. *[1] Microsoft Disclaimer*						
8.1.3	Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatie-beveiliging behoren te zijn vastgelegd.	Covered by ISO 27001:2013 and SOC 2	7.1.2	CC1.4	7.1.2	CC1.4	OST: Security – Human Resources Security; Privacy – Microsoft Personnel	
8.2.1	De directie behoort van werknemers, ingehuurd personeel en externe gebruikers te eisen dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de organisatie.	Covered by ISO 27001:2013 and SOC 2	7.2.1	CC2.2, CC2.3	7.2.1	CC2.2, CC2.3		
8.2.2	Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.	Covered by ISO 27001:2013 and SOC 2	7.2.2	CC2.2, CC2.4, CC3.2	7.2.2	CC2.2, CC2.4, CC3.2		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
8.2.3	Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die inbreuk op de beveiliging hebben gepleegd.	Covered by ISO 27001:2013 only	7.2.3	n/a	7.2.3	n/a		
8.2.3.1	Er is een disciplinair proces vastgelegd voor medewerkers die inbreuk maken op het beveiligings-beleid (zie ook: ARAR hoofdstuk VIII voor ambtenaren).	Covered by SOC 2 only	n/a	CC1.4	n/a	CC1.4		
8.3.1	De verantwoordelijkheden voor beëindiging of wijziging van het dienstverband behoren duidelijk te zijn vastgesteld en toegewezen.	Covered by ISO 27001:2013 and SOC 2	7.3.1	CC5.4	7.3.1	CC5.4		
8.3.2	Alle werknemers, ingehuurd personeel en externe gebruikers, behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband, contract of overeenkomst.	Covered by ISO 27001:2013 only	8.1.4	n/a	8.1.4	n/a		
8.3.3	De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie- en IT-voorzieningen, behoren te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoren na wijziging te worden aangepast.	Covered by ISO 27001:2013 and SOC 2	9.2.6	CC5.2	9.2.6	CC5.2		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
9.1.1	Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en IT-voorzieningen bevinden.	Covered by ISO 27001:2013 and SOC 2	11.1.1	n/a	11.1.1	n/a	MCIO SOC 2: CC5.5, CC5.6; OST: Physical and Environmental Security – Component Disposal	
9.1.1.5	Van ingehuurde bewakings-diensten is vooraf geverifieerd dat zij voldoen aan de wettelijke eisen gesteld in de Wet Particuliere Beveiligings-organisaties en Recherche-bureaus. Deze verificatie wordt minimaal jaarlijks herhaald.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
Detailed response of Microsoft regarding '9.1.1.5'		This control references regulation frameworks that are specific to The Netherlands. The Microsoft Online Services are an international infrastructure, we ask the reader to interpret this control in the BIR from an 'or equivalent' perspective. Microsoft screens personnel prior to providing access to customer data. The process for screening is available for review via a Microsoft representative. (Microsoft intranet document: https://microsoft.sharepoint.com/teams/Office 365sec/access/wiki/Pages/Clearance%20Requirements.aspx) Pursuant to local laws, regulations, ethics and contractual constraints, all Microsoft full-time employees (FTE) are required to successfully complete a standard background check as part of the hiring process. Background checks may include but are not limited to review of information relating to a candidate's education, employment, and criminal history. In the event that a vendor will be working with government data, Microsoft ensures that vendor companies perform the necessary background investigations on their personnel and report their findings annually. Microsoft data center personnel do not work with customer data as they have no access to customer data. *[1] Microsoft Disclaimer*						
9.1.2	Beveiligde zones behoren te worden beschermd door geschikte toegangs-beveiliging, om te bewerkstelligen dat alleen	Covered by ISO 27001:2013 and SOC 2	11.1.2	n/a	11.1.2	n/a	MCIO SOC 2: CC5.5, CC5.6; OST: Physical and Environmental Security –	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	bevoegd personeel wordt toegelaten.						Component Disposal	
9.1.2.2	De beveiligingszones en toegangsbeveiliging daarvan zijn ingericht conform het Kader Rijkstoegangsbeleid.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
Detailed response of Microsoft regarding '9.1.2.2'		This control references frameworks that are specific to The Netherlands Central Government. The Microsoft Online Services are an international infrastructure, we ask the reader to interpret this control in the BIR from an 'or equivalent' perspective. There are, in general, three zones inside each data center: public, office and production. Access control is implemented in each zone to protect the production environment. In data centers that Microsoft leases as a tenant, there will be physical segregation between Microsoft and other tenants to ensure proper physical protection. Microsoft Information Security Policy defines and establishes controls for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information. Access to media storage areas is restricted and audited. Access to all Microsoft buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into Data Centers. Front desk personnel are required to positively identify full-time employees (FTEs) or authorized contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. All guests are required to wear guest badges and be escorted by authorized Microsoft personnel. *[1] Microsoft Disclaimer*						
9.1.2.8	Er vindt minimaal één keer per half jaar een periodieke controle/evaluatie plaats op de autorisaties voor fysieke toegang.	Covered by SOC 2 only	n/a	n/a	n/a	CC5.2	MCIO SOC 2: CC5.5	
9.1.3	Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.	Covered by ISO 27001:2013 and SOC 2	11.1.3	n/a	11.1.3	n/a	MCIO SOC 2: CC5.5, CC5.6 OST: Physical and Environmental Security – Component Disposal	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
9.1.3.2	Er is actief beheer van sloten en kluizen met procedures voor wijziging van combinaties door middel van een sleutelplan. Opm.: het gaat hier alleen om daadwerkelijk gerubriceerde informatie.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
Detailed response of Microsoft regarding '9.1.3.2'		This control is interpreted as referencing physical locks, keys and vaults, to protect classified physical documents containing customer data. This is not applicable to the use of Microsoft Online Services. Microsoft does not print or receive any printed customer data in the data center. Our data center personnel do not have access to customer data and neither do they perform any operation on customer data. *[1] Microsoft Disclaimer*						
9.1.3.3	Serverruimtes, datacenters en daaraan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende best practices. Een goed voorbeeld van zo'n best practice is Telecommunication Infrastructure Standard for Data Centers (TIA-942).	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a	MOSC: 11.2.2, 11.2.3	
Detailed response of Microsoft regarding '9.1.3.3'		While Microsoft operates our program in alignment with the spirit of the ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centers, portions of the standard are not applicable to Microsoft or are in conflict with other regulatory and/or country specific requirements. As such, we currently do not certify to the standard. That being said, Microsoft does incorporate many of the industry leading practices outlined. Also see this whitepaper for more background information: http://download.microsoft.com/download/9/9/A/99ADCE75-5F63-4E47-905C-F511EE7D3786/Microsofts_Cloud_Networks_Strategy_Brief.pdf *[1] Microsoft Disclaimer*						
9.1.4	Er behoort fysieke bescherming tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vormen van natuurlijke of menselijke	Covered by ISO 27001:2013 and SOC 2	11.1.4	CC3.1, A1.2	11.1.4	CC3.1, A1.2		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	calamiteiten te worden ontworpen en toegepast.							
9.1.4.3	Beveiligde ruimten waarin zich bedrijfskritische apparatuur bevindt, zijn voldoende beveiligd tegen wateroverlast.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	MCIO SOC 2: CC6.1; FedRAMP: 13.11.14	
9.1.4.4	Bij het betrekken van nieuwe gebouwen wordt een locatie gekozen waarbij rekening wordt gehouden met de kans op en de gevolgen van natuurrampen en door mensen veroorzaakte rampen.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
Detailed response of Microsoft regarding '9.1.4.4'		The full selection criteria for the location of a new Microsoft Data Center are not available for review. The Microsoft Online Services and the data center infrastructure are designed for a guaranteed high availability and continuity of the services. External and environmental risks to the data center infrastructure are a factor in the risk analysis for location selection. Microsoft asks to review the available information on the Microsoft Online Services that document the data centers. Including the information available online: https://www.microsoft.com/en-us/cloud-platform/global-datacenters *[1] Microsoft Disclaimer*						
9.1.4.6	Er is door de brandweer goedgekeurde en voor de situatie geschikte brandblusapparatuur geplaatst en aangesloten. Dit wordt jaarlijks gecontroleerd.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a	MOSC: 11.2.2, 11.2.3	
Detailed response of Microsoft regarding '9.1.4.6'		Microsoft deploys approved fire detection and suppression equipment in the data center that activate automatically and notify designated organizations in the event of a fire. It is part of our physical and environmental protection controls. *[1] Microsoft Disclaimer*						
9.1.5	Er behoren fysieke bescherming en richtlijnen voor werken in beveiligde	Covered by ISO 27001:2013 and SOC 2	11.1.5	n/a	11.1.5	n/a	MCIO SOC 2: CC5.6; OST: Physical and Environmental	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	ruimten te worden ontworpen en toegepast.						Security – Component Disposal	
9.1.6	Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, behoren te worden beheerst en indien mogelijk te worden afgeschermd van IT-voorzieningen, om onbevoegde toegang te voorkomen.	Covered by ISO 27001:2013 and SOC 2	11.1.6	n/a	11.1.6	n/a	MCIO SOC 2: CC5.6; OST: Physical and Environmental Security – Component Disposal	
9.1.6.1	Er bestaat een procedure voor het omgaan met verdachte pakketten en brieven in postkamers en laad- en losruimten.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
9.2.1	Het voorkomen van verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten. Plaatsing en bescherming van apparatuur.	Covered by ISO 27001:2013 and SOC 2	11.2.1	A1.2	11.2.1	A1.2		
9.2.2	Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.	Covered by ISO 27001:2013 and SOC 2	11.2.2	A1.2	11.2.2	A1.2		
9.2.3	Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen	Covered by ISO 27001:2013 and SOC 2	11.2.3	A1.2	11.2.3	A1.2		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	interceptie of beschadiging te worden beschermd.							
9.2.4	Apparatuur behoort op correcte wijze te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.	Covered by ISO 27001:2013 and SOC 2	11.2.4	CC7.2, A1.2	11.2.4	CC7.2, A1.2		
9.2.4.1	Reparatie en onderhoud van apparatuur (hardware) vindt op locatie plaats door bevoegd personeel, tenzij er geen data op het apparaat aanwezig of toegankelijk is.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control. OST and MOSC cover a part of the control.	n/a	n/a	n/a	n/a	MOSC: A.11.2.4	
Detailed response of Microsoft regarding '9.2.4.1'		All repair and maintenance of equipment takes place onsite in the data center by approved third-party vendors following Microsoft's third-party management procedures. Also refer to A.11.2.4 Controls for equipment maintenance, A.11.2.5 Controls for removal of assets and A.11.2.6 Controls for security of equipment and assets off-premises. *[1] Microsoft Disclaimer*						
9.2.5	Apparatuur buiten de terreinen behoort te worden beveiligd, waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie.	Covered by ISO 27001:2013 and SOC 2	11.2.6	CC5.7	11.2.6	CC5.7		
9.2.6	Alle apparatuur die opslag-media bevat, behoort te worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn	Covered by ISO 27001:2013 and SOC 2	11.2.7	C1.3, CC5.7, C1.2	11.2.7	C1.3, CC5.7, C1.2		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	overschreven voordat de apparatuur wordt verwijderd.							
9.2.6.1	Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de beheerorganisatie ingeleverd. De beheer-organisatie zorgt voor een verantwoorde afvoer zodat er geen data op het apparaat aanwezig of toegankelijk is. Als dit niet kan, wordt het apparaat of de informatie-drager fysiek vernietigd. Het afvoeren of vernietigen wordt per bedrijfseenheid geregistreerd.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	MOSC: A.11.2.7; ISO27018: A.10.7; FedRAMP: 13.10.6	
9.2.6.2	Hergebruik van apparatuur buiten de organisatie is slechts toegestaan indien de informatie is verwijderd met een voldoende veilige methode. Een veilige methode is Secure Erase voor apparaten die dit ondersteunen. In overige gevallen wordt de data twee keer overschreven met vaste data, één keer met random data en vervolgens wordt geverifieerd of het overschrijven is gelukt.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	MOSC: A.11.2.7; ISO27018: A.10.7; FedRAMP: 13.10.6	
9.2.7	Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.	Covered by ISO 27001:2013 and SOC 2	11.2.5	CC5.7	11.2.5	CC5.7		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
10.1.1	Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben.	Covered by ISO 27001:2013 and SOC 2	12.1.1	CC3.2, CC5.7	12.1.1	CC3.2, CC5.7		
10.1.2	Wijzigingen in IT-voorzieningen en informatie-systemen behoren te worden beheerst.	Covered by ISO 27001:2013 and SOC 2	12.1.2	CC7.4	12.1.2	CC7.4		
10.1.2.2	Instellingen van informatie-beveiligingsfuncties (bijv. securitysoftware) op het koppelvlak tussen vertrouwde en on-vertrouwde netwerken, worden automatisch op wijzigingen gecontroleerd.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	13.1.1, 9.1.2	n/a	13.1.1, 9.1.2	n/a	FedRAMP: 13.1.4	
Detailed response of Microsoft regarding '10.1.2.2'		Forefront Identity Manager and IDS tools are implemented within the environment. Microsoft uses an Early Warning System (EWS) to support real-time analysis of events within its operational environment. Monitoring Agents and for example the Incident Management System generate near real-time alerts about events that could potentially compromise the system. Also refer to controls under A.12 and A.13, including A.12.2.1 Malware prevention controls and A.13.1.1 Controls for network management. *[1] Microsoft Disclaimer*						
10.1.3	Taken en verantwoordelijk-heidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Covered by ISO 27001:2013 and SOC 2	6.1.2	CC5.1	6.1.2	CC5.1		
10.1.3.2	Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheers-werkzaamheden worden	Covered by ISO 27001:2013 only	9.1.2, 9.2.3	n/a	9.1.2, 9.2.3	n/a	MOSC: 9.1.2	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.							
10.1.3.3	Vóór de verwerking van gegevens die de integriteit van kritieke informatie of kritieke informatiesystemen kunnen aantasten, worden deze gegevens door een tweede persoon geïnspecteerd en geaccepteerd. Van de acceptatie wordt een log bijgehouden.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
Detailed response of Microsoft regarding '10.1.3.3'	Microsoft Engineers do not have standing access to any service operation. All access is obtained through a rigorous access control technology called Lockbox. Today, Lockbox enforces access control through multiple levels of approval within Microsoft, providing just-in-time access with limited and time-bound authorization. In addition, all access control activities in the service are logged and audited. Microsoft follows NIST guidance regarding security considerations in software development in that information security must be integrated into the SDLC from system inception. Continual integration of security practices in the Microsoft SDL enables early identification and mitigation of security vulnerabilities and misconfigurations; awareness of potential software coding challenges caused by required security controls; identification of shared security services and reuse of security best practices tools which improve security posture through proven methods and techniques; and enforces Microsoft's already comprehensive risk management program. Microsoft has established software development and release management processes to control implementation of major changes including: • The identification and documentation of the planned change • Identification of business goals, priorities and scenarios during product planning • Specification of feature/component design • Operational readiness review based on a pre-defined criteria/check-list to assess overall risk/impact • Testing, authorization and change management based on entry/exit criteria for DEV (development), INT (Integration Testing), STAGE (Pre-production) and PROD (production) environments as appropriate Note that customers are responsible for their own applications hosted in Microsoft Azure. All changes into production go through the change management process. This process also requires that: • Pre-screened admin requests from Microsoft corporate networks are approved • That role-based and just-in-time access controls are enforced • Privileges issued are temporary and grant the least privilege required to complete task (just-enough access)						

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
		• Multi-factor authentication for all administrative access is required – All access requests are logged and audited *[1] Microsoft Disclaimer*						
10.1.3.4	Verantwoordelijkheden voor beheer en wijziging van gegevens en bijbehorende informatiesysteemfuncties moeten eenduidig toegewezen zijn aan één specifieke (beheerders)rol.	Covered by ISO 27001:2013 only	9.4.1	n/a	9.4.1	n/a	MOSC: 9.4.1	
10.1.4	Faciliteiten voor ontwikkeling, testen en productie behoren te zijn gescheiden om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.	Covered by ISO 27001:2013 and SOC 2	12.1.4	CC5.1, C1.1	12.1.4	CC5.1, C1.1		
10.1.4.3	Indien er een experimenteer- of laboratoriumomgeving is, is deze fysiek gescheiden van de productieomgeving.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a	MOSC: A.12.1.4	
Detailed response of Microsoft regarding '10.1.4.3'		Production and non-production are physically and logically separated. Microsoft employs network-based and host-based boundary protection devices such as firewalls, load balancers, IPFilters, jumpboxes and frontend components. These devices use mechanisms such as VLAN isolation, NAT and packet filtering to separate customer traffic from management traffic. Microsoft asks to review the available information on the Microsoft Online Services that document the Data Centers. Including the information available online: https://www.microsoft.com/en-us/cloud-platform/global-datacenters *[1] Microsoft Disclaimer*						
10.2.1	Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienst-verlening en niveaus van dienstverlening zoals	Covered by ISO 27001:2013 and SOC 2	15.1.1, 15.1.2, 15.2.1	CC2.2, CC2.3, C1.4	15.1.1, 15.1.2, 15.2.1	CC2.2, CC2.3, C1.4	OST: Use of Subcontractors	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	vastgelegd in de overeen-komst voor dienstverlening, door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.							
10.2.2	De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.	Covered by ISO 27001:2013 and SOC 2	15.2.1	C1.4, C1.5	15.2.1	C1.4, C1.5	OST: Microsoft Audits of Online Services	
10.2.3	Wijzigingen in de dienst-verlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatie-beveiliging, behoren te worden beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfs-systemen en -processen en met heroverweging van risico's.	Covered by ISO 27001:2013 and SOC 2	15.2.2	CC2.6, C1.6	15.2.2	CC2.6, C1.6		
10.3.1	Het gebruik van middelen behoort te worden gecontroleerd en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen, om de vereiste systeemprestaties te bewerkstelligen.	Covered by ISO 27001:2013 and SOC 2	12.1.3	A1.1, A1.2	12.1.3	A1.1, A1.2		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
10.3.1.1	De ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerk-stelligen. Op basis van een risico-analyse wordt bepaald wat de beschikbaarheidseis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen, op te vangen.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		To fulfill the requirements for this control, the customer is responsible for performing a risk assessment when adopting cloud services.
Detailed response of Microsoft regarding '10.3.1.1'		Microsoft data center Network architecture adopts Network Function Virtualization and Software Defined Networking. Microsoft asks to review the available information on the Microsoft Online Services that document the data centers. Including the information available online: https://www.microsoft.com/en-us/cloud-platform/global-datacenters *[1] Microsoft Disclaimer*						
10.3.1.2	Er worden beperkingen opgelegd aan gebruikers en systemen ten aanzien van	No direct ISO 27001:2013 control. SOC 2 does not provide	n/a	n/a	n/a	n/a		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	het gebruik van gemeen-schappelijke middelen, zodat een enkele gebruiker (of een enkel systeem) niet meer van deze middelen kan opeisen dan nodig is voor de uitvoering van zijn of haar taak en daarmee de beschikbaarheid van systemen voor andere gebruikers (of systemen) in gevaar kan brengen.	sufficient detail regarding this control.						
10.3.1.3	In koppelpunten met externe of onvertrouwde zones worden maatregelen getroffen om aanvallen te signaleren en hierop te reageren. Het gaat hier om aanvallen die erop gericht zijn de verwerkingscapaciteit zodanig te laten vollopen, dat onbereikbaarheid of uitval van computers het gevolg is (Denial of Service attacks).	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.16.4	
10.3.2	Er behoren aanvaardings-criteria te worden vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er behoort een geschikte test van het systeem of de systemen te worden uitgevoerd tijdens ontwikkeling en voorafgaand aan de acceptatie.	Covered by ISO 27001:2013 and SOC 2	14.2.9	CC7.1	14.2.9	CC7.1		
10.3.2.1	Van acceptatietesten wordt een log bijgehouden.	No direct ISO 27001:2013 control. SOC 2 does not provide	n/a	n/a	n/a	n/a		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
		sufficient detail regarding this control.						
Detailed response of Microsoft regarding '10.3.2.1'		Microsoft uses Secure Development Lifecycle (SDL) and Change Management procedures. Please refer to 10.1.3.3 *[1] Microsoft Disclaimer*						
10.4.1	Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.	Covered by ISO 27001:2013 and SOC 2	12.2.1	CC5.8	12.2.1	CC5.8	OST: Communications and Operations Management – Malicious Software	
10.4.1.1	Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, automatisch plaats.	Covered by SOC 2 and FedRAMP.	n/a	CC5.8	n/a	n/a	FedRAMP: 13.17.3	
10.4.1.2	Inkomende en uitgaande e-mails worden gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, (automatisch) plaats.	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a	Data Resiliency in Office 365	Azure: To fulfill the requirements for this control, the customer is responsible for ensuring that an e-mail service built on Azure is protected against viruses, trojans and other malware and that virus definitions are updated at least daily. Office 365: Exchange Online provides

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
								default functionality for protection of all e-mails against malware. Antivirus definitions are being updated at least daily. It is the customer's responsibility to make company-specific filtering customizations using the Exchange Admin Center; or to use additional antimalware/anti-phishing solutions for e-mails, such as the Exchange Online Advanced Threat Protection service for e-mail filtering, or other third-party antimalware solutions (e.g. sandboxing, end point protection, etc.).
10.4.1.4	Er zijn maatregelen om verspreiding van virussen tegen te gaan en daarmee schade te beperken (bijv. quarantaine en compartimentering).	Covered by SOC 2 and FedRAMP	n/a	CC5.8	n/a	n/a	FedRAMP: 13.17.3	
10.4.2	Als gebruik van 'mobile code' is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde 'mobile code' functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en behoort te worden	Covered by ISO 27001:2013 and SOC 2	12.2.1	CC5.8	12.2.1	CC5.8		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	voorkomen dat onbevoegde 'mobile code' wordt uitgevoerd.							
10.5.1	Er behoren back-upkopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig het vastgestelde back-upbeleid.	Covered by ISO 27001:2013 and SOC 2	12.3.1	A1.2, A1.3	12.3.1	A1.2, A1.3		
10.6.1	Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruik-maken van het netwerk, waaronder informatie die wordt getransporteerd.	Covered by ISO 27001:2013 and SOC 2	13.1.1	CC5.1, CC5.7	13.1.1	CC5.1, CC5.7		
10.6.1.2	Gegevensuitwisseling tussen vertrouwde en onvertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.17.3; MOSC: A.12.2.1	
10.6.1.3	Bij transport van vertrouwelijke informatie over onvertrouwde netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiertoe 12.3.1.3.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.1.13.2; MOSC: CA-44	
10.6.2	Beveiligingskenmerken, niveaus van dienstverlening en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en	Covered by ISO 27001:2013 and SOC 2	13.1.2	CC5.7	13.1.2	CC5.7		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	opgenomen in elke overeenkomst voor netwerk-diensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.							
10.7.1	Er behoren procedures te zijn vastgesteld voor het beheer van verwijderbare media.	Covered by ISO 27001:2013 and SOC 2	8.3.1	n/a	8.3.1	n/a	MCIO SOC 2: CC5.7; OST: Asset Management	
10.7.1.1	Er zijn procedures opgesteld en geïmplementeerd voor opslag van vertrouwelijke informatie voor verwijderbare media.	Covered by ISO 27001:2013, SOC 2 and FedRAMP	8.3.1	n/a	8.3.1	n/a	MCIO SOC 2: CC5.7; OST: Asset Management; FedRAMP: 13.10.7	
10.7.1.2	Verwijderbare media met vertrouwelijke informatie mogen niet onbeheerd worden achtergelaten op plaatsen die toegankelijk zijn zonder toegangscontrole.	Covered by ISO 27001:2013, SOC 2 and FedRAMP	8.3.1	n/a	8.3.1	n/a	MCIO SOC 2: CC5.7; OST: Asset Management; FedRAMP: 13.10.7	
10.7.2	Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Covered by ISO 27001:2013 and SOC 2	8.3.2	n/a	8.3.2	n/a	MCIO SOC 2: CC5.7; OST: Asset Management, Physical and Environmental Security – Component Disposal	
10.7.2.1	Er zijn procedures vastgesteld en in werking voor het verwijderen van vertrouwelijke data en de vernietiging van verwijder-bare media. Verwijderen van data wordt gedaan met een Secure Erase voor apparaten waar dit mogelijk is. In overige gevallen wordt de	Covered by FedRAMP only	n/a	n/a	n/a	n/a	MOSC: A.11.2.7; ISO 27018: A.10.7; FedRAMP: 13.10.6	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	data twee keer overschreven met vaste data, één keer met random data en vervolgens wordt geverifieerd of het overschrijven is gelukt. Zie ook 9.2.6.							
10.7.3	Er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik.	Covered by ISO 27001:2013 and SOC 2	8.2.3	CC5.1, CC5.7, A1.2	8.2.3	CC5.1, CC5.7, A1.2		
10.7.4	Systeemdocumentatie behoort te worden beschermd tegen onbevoegde toegang.	Covered by ISO 27001:2013 and SOC 2	14.1.1, 14.1.2, 14.1.3	CC5.1, CC5.7, A1.2	14.1.1, 14.1.2, 14.1.3	CC5.1, CC5.7, A1.2		
10.7.4.2	Wanneer de eigenaar er expliciet voor kiest om gerubriceerde systeemdocumentatie buiten de rijksdienst te brengen, doet hij dat niet zonder risicoafweging.	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		To fulfill the requirements for this control, the customer is responsible for ensuring that information owners perform risk assess-ments before deciding whether to share information outside of the controlled premises.
10.8.1	Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.	Covered by ISO 27001:2013 and SOC 2	13.2.1	CC5.7, C1.3	13.2.1	CC5.7, C1.3		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
10.8.1.1	Het meenemen van departementaal vertrouwelijke informatie buiten gecontroleerd gebied vindt uitsluitend plaats indien dit voor de uitoefening van de functie noodzakelijk is.	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		To fulfill the requirements for this control, the customer is responsible for ensuring that the use of departmental confidential information outside of the controlled premises only happens in order to perform a specific excercise by a specific function.
10.8.2	Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programma-tuur tussen de organisatie en externe partijen.	Covered by ISO 27001:2013 and SOC 2	13.2.2	C1.4	13.2.2	C1.4		
10.8.3	Media die informatie bevatten behoren te worden beschermd tegen onbevoegde toegang, misbruik of corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.	Covered by ISO 27001:2013 and SOC 2	8.3.3	n/a	8.3.3	n/a	MCIO SOC 2: CC5.7	
10.8.3.2	Fysieke verzending van bijzondere informatie dient te geschieden met ministerieel goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		This control is specifically aimed towards government agencies and the customer is responsible for fulfilling all requirements of the control.
10.8.4	Informatie die een rol speelt bij elektronische berichtuitwisseling behoort	Covered by ISO 27001:2013 and SOC 2	13.2.3	CC5.7	13.2.3	CC5.7		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	op geschikte wijze te worden beschermd.							
10.8.4.1	Digitale documenten binnen de rijksdienst waar eindgebruikers rechten aan kunnen ontlenen maken gebruik van PKI Overheid.	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		This control is specifically aimed towards government agencies and the customer is responsible for fulfilling all requirements of the control.
10.8.4.2	Er is een (spam)filter geactiveerd voor e-mailberichten.	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		Azure: To fulfill the requirements for this control, the customer is responsible for ensuring that an e-mail service built on Azure has an antispam filter. Office 365: Exchange Online provides default functionality for e-mail filtering. It is the responsibility of the customer to make company-specific filtering customiza-tions using the Exchange Admin Center; or to use additional (spam) filters.
10.8.5	Beleid en procedures behoren te worden ontwikkeld en geïmplementeerd om informatie te beschermen die een rol speelt bij de onderlinge koppeling van	Covered by ISO 27001:2013 and SOC 2	14.1.1, 14.1.2, 14.1.3	CC5.6	14.1.1, 14.1.2, 14.1.3	CC5.6		Office 365: Exchange Online provides default functionality for protection of all e-mails against malware. Antivirus definitions are being updated at least daily. It is the

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	systemen voor bedrijfsinformatie.							customer's responsibility to make company-specific filtering customizations using the Exchange Admin Center; or to use additional antimalware/antiphishing solutions for e-mails, such as the Exchange Online Advanced Threat Protection service for e-mail filtering, or other third-party antimalware solutions (e.g. sandboxing, end point protection, etc.)
10.9.1	Informatie die een rol speelt bij e-commerce en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaar-making en modificatie.	Covered by ISO 27001:2013 and SOC 2	14.1.2	CC5.7, PI1.3, PI1.5	14.1.2	CC5.7, PI1.3, PI1.5		
10.9.1.1	Waar mogelijk, worden authentieke basisregistraties van de overheid gebruikt (bijv. GBA).	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		This control is specifically aimed towards government agencies and the customer is responsible for fulfilling all requirements of the control.
10.9.2	Informatie die een rol speelt bij onlinetransacties behoort te worden beschermd om	Covered by ISO 27001:2013 and SOC 2	14.1.3	CC5.7, PI1.3	14.1.3	CC5.7, PI1.3		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking, onbevoegde duplicatie of onbevoegde weergave van berichten te voorkomen.							
10.9.3	De betrouwbaarheid van de informatie die beschikbaar wordt gesteld op een openbaar toegankelijk systeem, behoort te worden beschermd om onbevoegde modificatie te voorkomen.	Covered by ISO 27001:2013 and SOC 2	14.1.2	CC5.6, CC5.7	14.1.2	CC5.6, CC5.7		The second part of the control requires openly available information to be archived and an author of this information to be always mentioned within the text. It is the customer's responsibility to fulfill these requirements.
10.10.1	Activiteiten van gebruikers, uitzonderingen en informatiebeveiligings-gebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeen-gekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.	Covered by ISO 27001:2013 and SOC 2	12.4.1	CC6.2	12.4.1	CC6.2	OST: Communications and Operations Management – Event Logging	
10.10.1.2	Een logregel bevat minimaal: – een tot een natuurlijk persoon herleidbare gebruikersnaam of ID – de gebeurtenis (zie 10.10.2.1)	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	– waar mogelijk de identiteit van het werkstation of de locatie – het object waarop de handeling werd uitgevoerd – het resultaat van de handeling – de datum en het tijdstip van de gebeurtenis							
Detailed response of Microsoft regarding '10.10.1.2'		Logging of service, user and security events (web server logs, FTP server logs, etc.) is enabled and retained centrally. MCIO restricts access to audit logs to authorized personnel based on job responsibilities. Event logs are archived on OSSC's secure archival infrastructure and are retained for 180 days. 'Audit logging' is covered under the ISO 27001 standards and additional details can be found in the audit reports provided on the Azure Trust Center website. *[1] Microsoft Disclaimer*						
10.10.1.3	In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wacht-woorden, inbelnummers, etc.)	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
Detailed response of Microsoft regarding '10.10.1.3'		Microsoft Azure scrubs restricted data out of source code and log files. Restricted data includes personal identifiable information and credentials. *[1] Microsoft Disclaimer*						
10.10.1.4	Logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren aangesloten op een Security Information and Event Management-systeem (SIEM) waarmee meldingen en alarmoproepen aan de	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	beheerorganisatie gegeven worden. Er is vastgelegd bij welke drempelwaarden meldingen en alarm-oproepen gegenereerd worden.							
Detailed response of Microsoft regarding '10.10.1.4'		The customer can use a SIEM system to connect to the management of Microsoft Online Services. For example Office 365 has a Management Activity API. https://blogs.office.com/2015/04/21/announcing-the-new-office-365-management-activity-api-for-security-and-compliance-monitoring/ *[1] Microsoft Disclaimer*						
10.10.2	Er behoren procedures te worden vastgesteld om het gebruik van IT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.	Covered by ISO 27001:2013 and SOC 2	12.4.1	CC6.1, CC6.2	12.4.1	CC6.1, CC6.2		
10.10.3	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.	Covered by ISO 27001:2013 only	12.4.3	n/a	12.4.3	n/a		To fulfill the requirements for this control, the customer is responsible for ensuring protection of log data in Azure in case it has own access to log servers.
10.10.3.2	Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
Detailed response of Microsoft regarding '10.10.3.2'		Microsoft Engineers do not have standing access to any service operation. All access is obtained through a rigorous access control technology called Lockbox. Today, Lockbox enforces access control through multiple levels of approval within Microsoft, providing just-in-time access with limited and time-bound authorization. In addition, all access control activities in the service are logged and audited. Microsoft asks to review the available information on the Microsoft Online Services that document the data centers. Including the information available online: https://www.microsoft.com/en-us/cloud-platform/global-datacenters						

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
		[1] Microsoft Disclaimer						
10.10.3.5	De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de systeem-eigenaar. Bij een (vermoed) informatiebeveiligings-incident is de bewaartermijn minimaal drie jaar.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		To fulfill the requirements for this control, the customer is responsible for defining a log policy to maintain logs of Office 365 and Azure.
Detailed response of Microsoft regarding '10.10.3.5'		The customer can develop a policy on log archiving, for service logs that are under the customer's control/access. Logging of service, user and security events (web server logs, FTP server logs, etc.) is enabled and retained centrally. MCIO restricts access to audit logs to authorized personnel based on job responsibilities. Event logs are archived on OSSC's secure archival infrastructure and are retained for 180 days. 'Audit logging' is covered under the ISO 27001 standards and additional details can be found in the audit reports provided on the Azure Trust Center website. *[1] Microsoft Disclaimer*						
10.10.4	Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd.	Covered by ISO 27001:2013 only	12.4.3	n/a	12.4.3	n/a		
10.10.5	Storingen behoren in logbestanden te worden vastgelegd en te worden geanalyseerd en er behoren geschikte maatregelen te worden genomen.	Covered by ISO 27001:2013 only	12.4.1	n/a	12.4.1	n/a		
10.10.6	De klokken van alle relevante informatie-systemen binnen een organisatie of beveiligings-domein behoren te worden gesynchroniseerd met een	Covered by ISO 27001:2013 only	12.4.4	n/a	12.4.4	n/a		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	overeengekomen nauwkeurige tijdsbron.							
11.1.1	Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.	Covered by ISO 27001:2013 and SOC 2	9.1.1	CC5.1	9.1.1	CC5.1		
11.2.1	Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.	Covered by ISO 27001:2013 and SOC 2	9.2.1	CC5.2	9.2.1	CC5.2	OST: Access Control	To fulfill the requirements for this control, the customer is responsible for ensuring that their employees are registered and authorized prior to providing them with access.
11.2.1.2	Authenticatiegegevens worden bijgehouden in één bronbestand zodat consistentie is gegarandeerd.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.5.6.1	
11.2.1.3	Op basis van een risicoafweging wordt bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden verleend.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
11.2.2	De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.	Covered by ISO 27001:2013 and SOC 2	9.2.3	CC5.1	9.2.3	CC5.1		
11.2.3	De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.	Covered by ISO 27001:2013 and SOC 2	9.2.4	CC5.1	9.2.4	CC5.1		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
11.2.4	De directie behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces.	Covered by ISO 27001:2013 and SOC 2	9.2.5	CC5.4	9.2.5	CC5.4		To fulfill the requirements for this control, the customer is responsible for ensuring that user access rights are being reviewed.
11.3.1	Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden.	Covered by ISO 27001:2013 and SOC 2	9.3.1	CC5.1	9.3.1	CC5.1		
11.3.2	Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd.	Covered by ISO 27001:2013 only	11.2.8	n/a	11.2.8	n/a		
11.3.3	Er behoort een 'clear desk'-beleid voor papier en verwijderbare opslagmedia en een 'clear screen'-beleid voor IT-voorzieningen te worden ingesteld.	Covered by ISO 27001:2013 only	11.2.9	n/a	11.2.9	n/a		
11.3.3.3	Schermbeveiligings-programmatuur (een screensaver) maakt na een periode van inactiviteit van maximaal 15 minuten alle informatie op het beeldscherm onleesbaar en ontoegankelijk.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.1.11	
11.3.3.4	Toegangsbeveiliging-lock wordt automatisch geactiveerd bij het verwijderen van een token (indien aanwezig).	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		The customer is responsible for ensuring that access to its information systems is automatically disabled by the removal of access tokens.

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
11.4.1	Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze specifiek bevoegd zijn.	Covered by ISO 27001:2013 only	9.1.2	n/a	9.1.2	n/a		
11.4.2	Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen.	Covered by ISO 27001:2013 and SOC 2	9.1.2, 13.1.1, 13.1.2, 13.1.3	CC5.3	9.1.2, 13.1.1, 13.1.2, 13.1.3	CC5.3		
11.4.3	Automatische identificatie van apparatuur behoort te worden overwogen als methode om verbindingen vanaf specifieke locaties en apparatuur te authenticeren.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	OST: Asset Management; Azure – FedRAMP: 13.7.3 Device Identification and Authentication (IA-3)	
11.4.3.1	Alleen geïdentificeerde en geauthenticeerde apparatuur kan worden aangesloten op een vertrouwde zone. Eigen, ongeauthenticeerde apparatuur (BYOD – Bring Your Own Device) wordt alleen aangesloten op een onvertrouwde zone.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.1.15	
11.4.4	De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	Azure – FedRAMP: 13.1.3. Remote Access (AC-17); 13.1.4 Information Flow Enforcement (AC-4)	
11.4.5	Groepen informatiediensten, gebruikers en informatie-systemen behoren op netwerken te worden gescheiden.	Covered by ISO 27001:2013 and SOC 2	13.1.3	CC5.1, CC5.6	13.1.3	CC5.1, CC5.6	OST: Access Control – Network Design	
11.4.5.1	Werkstations worden zo ingericht dat routeren van verkeer tussen verschillende	No direct ISO 27001:2013 control. SOC 2	n/a	n/a	n/a	n/a	MOSC: A.13.1.3	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	zones of netwerken niet mogelijk is.	does not provide sufficient detail regarding this control. MOSC to cover a part of the control.						
11.4.5.2	De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument waarin is vastgelegd welke uitgangs-punten voor zonering worden gehanteerd. Van systemen wordt bijgehouden in welke zone ze staan. Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a	FedRAMP: 10.3	
11.4.5.3	Elke zone heeft een gedefinieerd beveiligings-niveau zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligings-niveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a	FedRAMP: 10.3	
11.4.5.4	Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail	n/a	n/a	n/a	n/a		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
		regarding this control.						
Detailed response of Microsoft regarding '11.4.5.1, 11.4.5.2, 11.4.5.3, 11.4.5.4'		Microsoft segregates groups of information services, users, and information systems on networks. The primary principle of network security is to allow only connection and communication that is necessary for system operation, blocking other ports, protocols, and connections by default. Data storage and processing is logically segregated among customers of the same service through the Active Directory structure and capabilities specifically developed to help build, manage, and secure multi-tenant environments. Also refer to A.13.1.3 Network segregation. *[1] Microsoft Disclaimer*						
11.4.6	Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de organisatie overschrijden, behoren de toegangs-mogelijkheden voor gebruikers te worden beperkt, overeenkomstig het toegangsbeleid en de eisen van bedrijfstoepassingen (zie 11.1).	Covered by ISO 27001:2013 and SOC 2	9.1.2, 13.1.1, 13.1.2, 13.1.3	CC5.1, CC5.3	9.1.2, 13.1.1, 13.1.2, 13.1.3	CC5.1, CC5.3		
11.4.7	Netwerken behoren te zijn voorzien van beheers-maatregelen voor netwerkroutering, om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoepassingen.	No direct ISO 27001:2013 control; SOC 2 does not provide sufficient detail regarding this control; other ISO 27001:2013 controls do not provide sufficient detail to completely cover this control. See FedRAMP for details on Azure information Flow Enforcement.	13.1.1, 9.1.2	n/a	13.1.1, 9.1.2	n/a	Azure – FedRAMP: 13.1.4 Information Flow Enforcement (AC-4)	Microsoft offers a penetration testing and Bug Bounty program for both Azure and Office 365. Reports are available in the Microsoft Service Trust Portal (https://aka.ms/stp).

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
Detailed response of Microsoft regarding '11.4.7'		Network routing control is generally covered by controls implemented by Microsoft as part of several (other) control objectives. The controls are verified under SOC, ISO or FedRAMP compliance by third parties, as stated in the compliance reports. For this control, Microsoft refers to the following information, which is accessible through the Service Assurance tab of the Office 365 Security & Compliance Portal: • Implementation and testing details of ISO 27001:2013 control, 13.1.1, A.9.1.2, 12.1.4; • Microsoft's responses to control DSI02 in the document "Office 365 Mapping of CSA Cloud Control Matrix 3.0.1". More detail and relevant citations: [ISO 13.1.1] *Microsoft manages and controls networks to protect information in systems and applications. Microsoft protects the confidentiality and integrity of transmitted information. Multiple techniques are used to control information flows, including but not limited to:* • *Physical separation: Network segments are physically separated by routers that are configured to prevent specific communication patterns.* • *Logical separation: Virtual LAN (VLAN) technology is used to further separate communications.* • *Firewalls: Firewalls and other network security enforcement points are used to limit data exchanges with systems that are exposed to the internet, and to isolate front-end systems from back-end systems managed by Office 365.* • *Protocol restrictions: traffic to and from customers is transmitted over encrypted connections. Microsoft implements boundary protection through the use of controlled devices at the network boundary and at key points within the network.* *The primary goal of network security is to allow only connections and communications that are necessary for system operation; blocking other ports, protocols and connections by default. Access Control Lists (ACLs) are the preferred mechanism to restrict network communications by source and destination networks, ports and protocols. Approved mechanisms to implement networked-based ACLs include: Tiered ACLs on routers managed by Microsoft's Cloud Infrastructure & Operations (MCIO) team, IPsec policies applied to hosts to restrict communications (when used in conjunction with tiered ACLs), firewall rules, and host-based firewall rules.* *Microsoft implements information flow control by allowing only connections and communication that are necessary to allow system operation, blocking other ports, protocols and connections by default, as defined in Microsoft's Online Services security standard. Microsoft manages ACL approvals through a Request for Change process (that includes review and risk acceptance) and MCIO implements the approved change.* [CSA DSI02] *Office 365 has documented and maintains a data flow diagram which accounts for all system connections, the ports and protocols those connections use to communicate, and the classification of data flowing through the connections. The data flow diagram documents inner-system connections and also documents connections with third parties. The Office 365 Security Policy requires that this documentation is reviewed and updated regularly.* Microsoft Azure also implements ISO 27001:2013 and uses MCIO for hardware operations as well. *[1] Microsoft Disclaimer*						
11.5.1	Toegang tot besturings-systemen behoort te worden beheerst met een beveiligde inlogprocedure.	Covered by ISO 27001:2013 and SOC 2	9.4.2	CC5.1	9.4.2	CC5.1		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
11.5.1.1	Toegang tot kritieke toepassingen of toepassingen met een hoog belang wordt verleend op basis van two-factor authenticatie.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.1.9	
11.5.1.5	Nadat voor een gebruikers-naam 5 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lockout-periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lockout op te heffen of het wachtwoord te resetten.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.1.7, 13.1.9	
11.5.2	Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.	Covered by ISO 27001:2013 and SOC 2	9.2.1	CC5.3	9.2.1	CC5.3		
11.5.2.3	Applicaties mogen niet onnodig en niet langer dan noodzakelijk onder een systeemaccount (een privileged user zoals administrator of root) draaien. Direct na het uitvoeren van handelingen waar hogere rechten voor nodig zijn, wordt weer teruggeschakeld naar het niveau van een gewone	No direct ISO 27001:2013 control; SOC 2 does not provide sufficient detail regarding this control; other ISO 27001:2013 controls do not provide sufficient detail to completely cover this control.	9.4.1	n/a	9.4.1	n/a		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	gebruiker (een unprivileged user).							
Detailed response of Microsoft regarding '11.5.2.3'		Use of system tooling is generally covered by controls implemented by Microsoft as part of several (other) control objectives. The controls are verified under SOC, ISO or FedRAMP compliance by third parties, as stated in the compliance reports. For this control, Microsoft refers to the following information, which is accessible through the Service Assurance tab of the Office 365 Security & Compliance Portal: • Implementation and testing details of ISO 27001:2013 control, 9.4.1. More detail and relevant citations: [ISO 9.4.1] *Microsoft restricts access to Office 365 information and application system functions in accordance with an access control policy. The Office 365 system enforces role-based access control over all subjects and objects specified by the policy. The policy is uniformly enforced across subjects and objects within the boundary of the information system. All Office 365 accounts are considered privileged. Each Office 365 administrator is assigned a role within their team that corresponds to a security group. Each security group is assigned permissions to correlating environments with just enough access to properly fulfill their tasks. Office 365 teams use the concept of least privilege, allowing only pre-authorized accesses for administrators which are necessary to accomplish assigned tasks in accordance with business functions and organizational needs along with just-in-time access enforcements. 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. Furthermore, an access control tool sits between the administrator and the customer's data. The tool checks the scope of the administrator's permissions for carrying out certain activities. The tool will approve or deny the request and, if approved, grant access only after management approval has also been obtained. In certain situations, the tool may also call on another administrator to assist with the situation. Only absolutely necessary actions are permitted, and access is granted on a time-limited basis. After the permitted entry period has expired, access privileges are automatically revoked. Every request for elevated privileges is logged.* *[1] Microsoft Disclaimer*						
11.5.3	Systemen voor wachtwoord-beheer behoren interactief te zijn en moeten bewerkstelligen dat wacht-woorden van geschikte kwaliteit worden gekozen.	Covered by ISO 27001:2013 and SOC 2	9.4.3	CC5.1	9.4.3	CC5.1		
11.5.3.2	Wachtwoorden hebben een geldigheidsduur van maximaal 3 maanden. Daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is,	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.1.9	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	wordt het account geblokkeerd.							
11.5.3.3	Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een zeer beperkte geldigheidsduur en moeten bij het eerste gebruik worden gewijzigd.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.7.5	
11.5.4	Het gebruik van hulp-programmatuur waarmee systeem- en toepassings-beheersmaatregelen zouden kunnen worden gepasseerd, behoort te worden beperkt en behoort strikt te worden beheerst.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
Detailed response of Microsoft regarding '11.5.4'		Use of system tooling is generally covered by controls implemented by Microsoft as part of several (other) control objectives. The controls are verified under SOC, ISO or FedRAMP compliance by third parties, as stated in the compliance reports. For this control, Microsoft refers to the following information, which is accessible through the Service Assurance tab of the Office 365 Security & Compliance Portal: • Implementation and testing details of ISO 27001:2013 control, 9.4.1. More detail and relevant citations: [ISO 9.4.1] *Microsoft restricts access to Office 365 information and application system functions in accordance with an access control policy. The Office 365 system enforces role-based access control over all subjects and objects specified by the policy. The policy is uniformly enforced across subjects and objects within the boundary of the information system. All Office 365 accounts are considered privileged. Each Office 365 administrator is assigned a role within their team that corresponds to a security group. Each security group is assigned permissions to correlating environments with just enough access to properly fulfill their tasks. Office 365 teams use the concept of 'least privilege', allowing only pre-authorized accesses for administrators which are necessary to accomplish assigned tasks in accordance with business functions and organizational needs along with just-in-time access enforcements. 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. Furthermore, an access control tool sits between the administrator and the customer's data. The tool checks the scope of the administrator's permissions for carrying out certain activities. The tool will approve or deny the request and, if approved, grant access only after management approval has also been obtained. In certain situations, the tool may also call on another administrator to assist with the situation. Only absolutely necessary actions are permitted, and access is granted on a time-limited basis. After the permitted entry period has expired, access privileges are automatically revoked. Every request for elevated privileges is logged.*						

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
		[1] Microsoft Disclaimer						
11.5.5	Inactieve sessies behoren na een vastgestelde periode van inactiviteit te worden uitgeschakeld.	No direct ISO 27001:2013 control, SOC 2 does not provide sufficient detail regarding this control; see FedRAMP for details on Azure devices identification and authentication	n/a	n/a	n/a	n/a	Azure – FedRAMP: 13.1.11 Session Termination (AC-12)	
Detailed response of Microsoft regarding '11.5.5'		Session time-out is generally covered by controls implemented by Microsoft as part of several (other) control objectives. The controls are verified under SOC, ISO or FedRAMP compliance by third parties, as stated in the compliance reports. For this control, Microsoft refers to the following information, which is accessible through the Service Assurance tab of the Office 365 Security & Compliance Portal: • Implementation and testing details of ISO 27001:2013 control, 11.2.8. More detail and relevant citations. [ISO 11.2.8]: *Microsoft prevents access to the system by initiating a session lock after a period of inactivity or upon receiving a request from a user. Microsoft has implemented policies that enforce session time-out requirements in Office 365.* *[1] Microsoft Disclaimer*						
11.5.5.1	De periode van inactiviteit van een werkstation is vastgesteld op maximaal 15 minuten. Daarna wordt de PC vergrendeld. Bij remote-desktopsessies geldt dat de sessie na maximaal 15 minuten inactiviteit verbroken wordt.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.1.10	
11.5.6	De verbindingstijd behoort te worden beperkt als aanvullende beveiliging voor	No direct ISO 27001:2013 control, SOC 2 does not provide	n/a	n/a	n/a	n/a	Azure – FedRAMP: 13.1.3 Access Enforcement (AC-3) Microsoft Azure	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	toepassingen met een verhoogd risico.	sufficient detail regarding this control; see FedRAMP for details on Azure administrators finite access to Azure production environment.					Just in Time (JIT) administrator access to the production environment	
Detailed response of Microsoft regarding '11.5.6'		Connection time control is generally covered by controls implemented by Microsoft as part of several (other) control objectives. The controls are verified under SOC, ISO or FedRAMP compliance by third parties, as stated in the compliance reports. For this control, Microsoft refers to the following information, which is accessible through the Service Assurance tab of the Office 365 Security & Compliance Portal: • Implementation and testing details of ISO 27001:2013 control, 9.4.1; • FedRAMP Azure SSP, control AC-3. More detail and relevant citations: [ISO 9.4.1] *Microsoft restricts access to Office 365 information and application system functions in accordance with an access control policy. The Office 365 system enforces role-based access control over all subjects and objects specified by the policy. The policy is uniformly enforced across subjects and objects within the boundary of the information system. All Office 365 accounts are considered privileged. Each Office 365 administrator is assigned a role within their team that corresponds to a security group. Each security group is assigned permissions to correlating environments with just enough access to properly fulfill their tasks. Office 365 teams use the concept of 'least privilege', allowing only pre-authorized accesses for administrators which are necessary to accomplish assigned tasks in accordance with business functions and organizational needs along with just-in-time access enforcements. 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. Furthermore, an access control tool sits between the administrator and the customer's data. The tool checks the scope of the administrator's permissions for carrying out certain activities. The tool will approve or deny the request and, if approved, grant access only after management approval has also been obtained. In certain situations, the tool may also call on another administrator to assist with the situation. Only absolutely necessary actions are permitted, and access is granted on a time-limited basis. After the permitted entry period has expired, access privileges are automatically revoked. Every request for elevated privileges is logged.* *[1] Microsoft Disclaimer*						
11.5.6.1	De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis van een wijzigingsverzoek of storingsmelding.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.1.2.2	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
11.6.1	Toegang tot informatie en functies van toepassings-systemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangs-beleid.	Covered by ISO 27001:2013 and SOC 2	9.4.1	CC5.1, CC7.1	9.4.1	CC5.1, CC7.1		
11.6.1.2	Managementsoftware heeft de mogelijkheid gebruikers-sessies af te sluiten.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
Detailed response of Microsoft regarding '11.6.1.2'		Microsoft Engineers do not have standing access to any service operation. All access is obtained through a rigorous access control technology called Lockbox. Lockbox enforces access control through multiple levels of approval within Microsoft, providing just-in-time access with limited and time-bound authorization. In addition, all access control activities in the service are logged and audited. Also see detailed response of Microsoft regarding 11.5.4. *[1] Microsoft Disclaimer*						
11.6.1.3	Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.1.9	
11.6.1.4	Een beheerder gebruikt two-factor authenticatie voor het beheer van kritieke apparaten. Bijv. een sleutel tot beveiligde ruimte en een password of een token en een password.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
Detailed response of Microsoft regarding '11.6.1.4'		Microsoft Azure enforces the concept of 'least privilege' and restricts access to information systems, including the hypervisor or hypervisor management plane using role-based security groups. All management access requires multi-factor authentication, and all access is logged. *[1] Microsoft Disclaimer*						

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
11.6.2	Gevoelige systemen behoren een eigen, vast toegewezen (geïsoleerde) computeromgeving te hebben.	Covered by ISO 27001:2013, SOC 2 and FedRAMP	13.1.3	CC5.1, CC5.6	13.1.3	CC5.1, CC5.6	FedRAMP: 10.3.5	
11.6.2.1	Gevoelige systemen (met hoge beschikbaarheid of grote vertrouwelijkheid) behoren een eigen vast toegewezen (geïsoleerde) computeromgeving te hebben. Isoleren kan worden bereikt door fysieke of logische methoden.	Covered by ISO 27001:2013 and SOC 2	13.1.3	CC5.1, CC5.6	13.1.3	CC5.1, CC5.6		
11.7.1	Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.	Covered by ISO 27001:2013 only	6.2.1	n/a	6.2.1	n/a		
11.7.1.1	Het mobiele apparaat is waar mogelijk zo ingericht dat geen bedrijfsinformatie wordt opgeslagen ('zero footprint'). Voor het geval dat zero footprint (nog) niet realiseerbaar is – of functioneel onwenselijk is – geldt: een mobiel apparaat (zoals een handheld computer, tablet, smart-phone, PDA) biedt de mogelijkheid om de toegang te beschermen d.m.v. een wachtwoord en versleuteling van die gegevens.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.1.15	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	Voor printen in on-vertrouwde omgevingen vindt een risicoafweging plaats.							
11.7.1.2	Er zijn, waar mogelijk, voorzieningen om de actualiteit van anti-malwareprogrammatuur op mobiele apparaten te garanderen.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.1.15	
11.7.1.3	Bij melding van verlies of diefstal wordt de communicatiemogelijkheid met de centrale applicaties afgesloten.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
Detailed response of Microsoft regarding '11.7.1.3'		Wireless / mobile access to production networks is not permitted within the data centers. The concept of a 'device with administrative access' is not applicable. *[1] Microsoft Disclaimer*						
11.7.2	Er behoren beleid, operationele plannen en procedures voor telewerken te worden ontwikkeld en geïmplementeerd.	Covered by ISO 27001:2013 only	6.2.2	n/a	6.2.2	n/a		
11.7.2.2	De telewerkvoorzieningen zijn waar mogelijk zo ingericht dat op de werkplek (thuis of op een andere locatie) geen bedrijfs-informatie wordt opgeslagen ('zero footprint') en mogelijke malware vanaf de werkplek niet in het vertrouwde deel terecht kan komen. Voor printen in on-vertrouwde omgevingen	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.1.13	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	vindt een risicoafweging plaats.							
12.1.1	In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligings-maatregelen te worden opgenomen	Covered by ISO 27001:2013 and SOC 2	14.1.1	CC3.2, CC7.1	14.1.1	CC3.2, CC7.1		
12.2.1	Gegevens die worden ingevoerd in toepassingen behoren te worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn.	Covered by SOC 2 only	n/a	PI1.2	n/a	PI1.2		To fulfill the requirements for this control, the customer is responsible for ensuring that data is correctly entered in MS Online Services.
12.2.2	Er behoren validatiecontroles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken.	Covered by ISO 27001:2013 and SOC 2	16.1.4	PI1.3, PI1.5	16.1.4	PI1.3, PI1.5		
12.2.3	Er behoren eisen en geschikte beheers-maatregelen te worden vastgesteld en geïmplementeerd voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.	Covered by ISO 27001:2013 and SOC 2	9.1.2, 9.2.4, 9.4.1	PI1.2, PI1.3, PI1.5	9.1.2, 9.2.4, 9.4.1	PI1.2, PI1.3, PI1.5		
12.2.4	Gegevensuitvoer uit een toepassing behoort te worden gevalideerd, om te bewerkstelligen dat de verwerking van opgeslagen gegevens op de juiste	Covered by SOC 2 only	n/a	PI1.5	n/a	PI1.5		To fulfill the requirements for this control, the customer is responsible for ensuring that data is correctly validated

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	manier plaatsvindt en geschikt is gezien de omstandigheden.							when exported and identifiable by the user of the data.
12.2.4.3	Alleen gegevens die noodzakelijk zijn voor de doeleinden van de gebruiker worden uitgevoerd (need to know).	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 13.1.6	
12.3.1	Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.	Covered by ISO 27001:2013 only	10.1.1	n/a	10.1.1	n/a		To fulfill the requirements for this control when using Microsoft Azure, the customer is responsible for enabling encryption and maintain key management within the solution. When using Microsoft Office 365, Customer Lockbox functionality can be used to limit the ability of Microsoft to access customer data.
12.3.1.3	De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2 en waar mogelijk NBV).	Covered by FedRAMP only	n/a	n/a	n/a	n/a	FedRAMP: 10.7.1	
12.3.2	Er behoort sleutelbeheer te zijn vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.	Covered by ISO 27001:2013 only	10.1.2	n/a	10.1.2	n/a		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
12.3.2.5	Bij voorkeur is sleutelmanagement ingericht volgens PKI Overheid.	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		This control is specifically aimed towards government agencies and the customer is responsible for fulfilling all requirements of the control.
12.4.1	Er behoren procedures te zijn vastgesteld om de installatie van programmatuur op productiesystemen te beheersen.	Covered by ISO 27001:2013 only	12.5.1	n/a	12.5.1	n/a		
12.4.2	Testgegevens behoren zorgvuldig te worden gekozen, beschermd en beheerst.	Covered by ISO 27001:2013 and SOC 2	14.3.1	CC7.1, C1.2	14.3.1	CC7.1, C1.2		To fulfill the requirements for this control, the customer is responsible for ensuring that data is not used in test environments.
12.4.3	De toegang tot broncode van programmatuur behoort te worden beperkt.	Covered by ISO 27001:2013 only	9.4.5	n/a	9.4.5	n/a		
12.5.1	De implementatie van wijzigingen behoort te worden beheerst door middel van formele procedures voor wijzigingsbeheer.	Covered by ISO 27001:2013 and SOC 2	14.2.2	CC7.3, CC7.4	14.2.2	CC7.3, CC7.4		
12.5.2	Bij wijzigingen in besturings-systemen behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie.	Covered by ISO 27001:2013 and SOC 2	14.2.3	CC7.4	14.2.3	CC7.4		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
12.5.3	Wijzigingen in programmatuurpakketten behoren te worden ontmoedigd en te worden beperkt tot noodzakelijke wijzigingen, en alle wijzigingen behoren strikt te worden beheerst.	Covered by ISO 27001:2013 and SOC 2	14.2.4	CC7.4	14.2.4	CC7.4		
12.5.4	Er behoort te worden voorkomen dat zich gelegenheden voordoen om informatie te laten uitlekken.	Covered by OST only. In general, ISO 27001:2013 and SOC 2 certifications demonstrate MS measures to prevent information leakage.	n/a	n/a	n/a	n/a	OST: General Privacy and Security Terms – Security; Data Processing Terms – Privacy, Security	When using Microsoft Azure, consider preventive measures such as data leakage prevention software for critical applications and monitor the environment continuously. When using Microsoft Office 365, ensure that the configurations for information sharing are in line with the security policy and data leakage prevention settings are configured where possible.
12.5.5	Uitbestede ontwikkeling van programmatuur behoort onder supervisie te staan van en te worden gecontroleerd door de organisatie.	Covered by ISO 27001:2013 and SOC 2	14.2.7	CC2.1, CC7.1	n/a	CC2.1, CC7.1		
12.6.1	Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatie-systemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden	Covered by ISO 27001:2013 and SOC 2	12.6.1	CC6.1	12.6.1	CC6.1		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.							
12.6.1.4	Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is, worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritieke beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
Detailed response of Microsoft regarding '12.6.1.4'		Procedures have been established and implemented to scan for vulnerabilities on MCIO-managed hosts in the scope boundary. MCIO implements vulnerability scanning on server operating systems, databases, and network devices with appropriate vulnerability scanning tool. MCIO web applications are scanned with the appropriate scanning solution. The vulnerability scans are performed on a monthly basis at minimum. Microsoft Azure contracts with independent assessors to perform penetration testing of the Microsoft Azure boundary. Software updates are released through the monthly OS release cycle using change and release management procedures. Emergency out-of-band security software updates (0-day & Software Security Incident Response Process – SSIRP updates) are deployed as quickly as possible. If customers use the default 'Auto Upgrade' option, software updates will be applied to their VMs automatically. Otherwise, customers have the option to upgrade to the latest OS image through the portal. In case of a VM role, customers are responsible for evaluating and updating their VMs. Office 365 identifies, reports, and corrects information system flaws through vulnerability management, incident response management, and patch/configuration management processes. The Office 365 Security Incident Response Program assists with identifying and reporting of information system flaws. Office 365 MT 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. All customers, including government and non-government customers, are responsible for ensuring that customer users are using secure browsers and properly patched information systems. *[1] Microsoft Disclaimer*						

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
13.1.1	Informatiebeveiligings-gebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	Covered by ISO 27001:2013 and SOC 2	16.1.2	CC6.2	16.1.2	CC6.2		
13.1.1.2	Er is een contactpersoon aangewezen voor het rapporteren van beveiligings-incidenten. Voor integriteits-schendingen is ook een vertrouwenspersoon aangewezen die meldingen in ontvangst neemt.	No direct ISO 27001:2013 control. SOC 2 does not provide sufficient detail regarding this control.	n/a	n/a	n/a	n/a		
Detailed response of Microsoft regarding '13.1.1.2'		Procedures require reporting incidents to the Investigation and Response team. Security awareness training includes content, related to recognizing and reporting potential indicators of insider threat. *[1] Microsoft Disclaimer*						
13.1.1.4	Informatie over de beveiligingsrelevante handelingen van de gebruiker wordt regelmatig nagekeken. De BVA bekijkt maandelijks een samenvatting van de informatie.	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		To fulfill the requirements for this control, the customer is responsible for ensuring that the user actions audit logs of Azure and Office 365 are being reviewed periodically.
13.1.2	Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en -diensten behoort te worden geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren.	Covered by ISO 27001:2013 and SOC 2	16.1.3	CC6.1	16.1.3	CC6.1		
13.2.1	Er behoren leidinggevende verantwoordelijkheden en procedures te worden vastgesteld om een snelle,	Covered by ISO 27001:2013 and SOC 2	16.1.1	CC6.2	16.1.1	CC6.2		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	doeltreffende en ordelijke reactie op informatie-beveiligingsincidenten te bewerkstelligen.							
13.2.2	Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligings-incidenten kunnen worden gekwantificeerd en gecontroleerd.	Covered by ISO 27001:2013 and SOC 2	16.1.6	CC6.2	16.1.6	CC6.2		
13.2.3	Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligings-incident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeen-komstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.	Covered by ISO 27001:2013 and SOC 2	16.1.7	CC6.2	16.1.7	CC6.2		
14.1.1	Er behoort een beheerd proces voor bedrijfs-continuïteit in de gehele organisatie te worden ontwikkeld en bijgehouden, voor de naleving van eisen voor informatiebeveiliging die nodig zijn voor de continuïteit van de bedrijfsvoering.	Covered by ISO 27001:2013 and SOC 2	17.1.2	A1.2	17.1.2	A1.2		
14.1.1.1	Calamiteitenplannen worden jaarlijks gebruikt in bewustwordings-, trainings- en testactiviteiten.	Covered by SOC 2 and FedRAMP	n/a	A1.1	n/a	A1.1	FedRAMP: 13.6.3	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
14.1.2	Gebeurtenissen die tot onderbreking van bedrijfs-processen kunnen leiden, behoren te worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor informatie-beveiliging.	Covered by ISO 27001:2013 and SOC 2, with exception of Recovery Point Objective (RPO) and Recovery Time Objective (RTO)	17.1.1	A1.2, A1.3, CC3.3	17.1.1	A1.2, A1.3, CC3.3		
Detailed response of Microsoft regarding '14.1.2'		Business Continuity is generally covered by controls implemented by Microsoft as part of several (other) control objectives. The controls are verified under SOC, ISO or FedRAMP compliance by third parties, as stated in the compliance reports. For this control, Microsoft refers to the following information, which is accessible through the Service Assurance tab of the Office 365 Security & Compliance Portal: • Implementation details controls ISO 17.1.1, 12.3.1 and SOC A1.1, A1.2, CC3.3 • Microsoft's responses to control BCR-02 in the document "Office 365 Mapping of CSA Cloud Control Matrix 3.0.1", which provides some context on the internal use of RPO/RTO • White paper "Data resiliency in Office 365", February 2016 More detail and relevant citations: Any loss of availability is measured by the financially backed Service Level Agreements that Microsoft provides. The way Microsoft Office 365 is architected (see referenced white paper), by also implementing availability at the application layer, negates the suitability of publishing RPO and RTO values as a measure for system recoverability. However, internal objectives are zero downtime and zero data loss. Microsoft is strongly committed to keeping data safe and is certified against ISO 27001 and SOC 2 inter alia, both of which require attention to service continuity planning. Microsoft states in our responses to control BCR-02 in the document "Office 365 Mapping of CSA Cloud Control Matrix 3.0.1". [CSA BCR-02] *Business Continuity Plans (BCPs) are documented and reviewed at least annually. The BCPs provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).* *The Business Continuity team in coordination with the Office 365 service teams conduct testing of the business continuity and disaster recovery plans at least annually. Testing ensures that each loss scenario is tested at least annually. Issues identified during testing are noted and managed to resolution by the Office 365 service team in coordination with the Business Continuity team.* *[1] Microsoft Disclaimer*						
14.1.3	Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te	Covered by ISO 27001:2013 and SOC 2	17.1.2	A1.2	17.1.2	A1.2		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	handhaven of te herstellen en om de beschikbaarheid van informatie op het vereiste niveau en in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritieke bedrijfsprocessen.							
14.1.4	Er behoort een enkelvoudig kader voor bedrijfs-continuïteitsplannen te worden gehandhaafd om te bewerkstelligen dat alle plannen consistent zijn, om eisen voor informatie-beveiliging op consistente wijze te behandelen en om prioriteiten vast te stellen voor testen en onderhoud.	Covered by ISO 27001:2013 and SOC 2	17.1.2	A1.2	17.1.2	A1.2		
14.1.5	Bedrijfscontinuïteitsplannen behoren regelmatig te worden getest en geüpdatet, om te bewerkstelligen dat ze actueel en doeltreffend blijven.	Covered by ISO 27001:2013 and SOC 2	17.1.3	A1.3	17.1.3	A1.3		
14.1.5.1	Er worden minimaal jaarlijks oefeningen en testen gehouden om de bedrijfs-continuïteitsplannen en de mate van readiness van de organisatie te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.	Covered by SOC 2 and FedRAMP	n/a	A1.1	n/a	A1.1	FedRAMP: 13.6.3	
15.1.1	Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen	Covered by ISO 27001:2013 and SOC 2	18.1.1	CC3.3	18.1.1	CC3.3		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	en de benadering van de organisatie in de naleving van deze eisen, behoren expliciet te worden vastgesteld, gedocumenteerd en actueel te worden gehouden voor elk informatiesysteem en voor de organisatie.							
15.1.2	Er behoren geschikte procedures te worden geïmplementeerd om te bewerkstelligen dat wordt voldaan aan de wettelijke en regelgevende eisen en contractuele verplichtingen voor het gebruik van materiaal waarop intellectuele eigendoms-rechten kunnen berusten en het gebruik van programmatuur waarop intellectuele eigendoms-rechten berusten.	Covered by ISO 27001:2013 only	18.1.2	n/a	18.1.2	n/a		
15.1.3	Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.	Covered by ISO 27001:2013 and SOC 2	18.1.3	n/a	18.1.3	n/a	OST: Customer Data Deletion or Return; MCIO SOC 2: C11.2.7	To fulfill the requirements for this control, the customer is responsible for ensuring that PII is not kept longer than required at Microsoft Online Services.
15.1.4	De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.	Covered by ISO 27001:2013 only	18.1.4	n/a	18.1.4	n/a	OST: Bekendmaking van Gegevens van de Klant; ISO27018	

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
15.1.5	Gebruikers behoren ervan te worden weerhouden IT-voorzieningen te gebruiken voor onbevoegde doeleinden.	Covered by SOC 2 only	n/a	CC1.3, CC1.4	n/a	CC1.3, CC1.4		
15.1.6	Cryptografische beheers-maatregelen behoren overeenkomstig alle relevante overeenkomsten, wetten en voorschriften te worden gebruikt.	Covered by ISO 27001:2013 only	18.1.5	n/a	18.1.5	n/a		
15.2.1	Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijk-heid vallen correct worden uitgevoerd om naleving te bereiken van beveiligings-beleid en -normen.	Covered by ISO 27001:2013 only	18.2.2	n/a	18.2.2	n/a		
15.2.1.2	In de P&C-cyclus wordt gerapporteerd over informatiebeveiliging aan de hand van het 'in control'-statement.	No responsibilities for Microsoft regarding this control	n/a	n/a	n/a	n/a		This control is specifically aimed towards government agencies and the customer is responsible for fulfilling all requirements of the control.
15.2.2	Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen.	Covered by ISO 27001:2013 only	18.2.3	n/a	18.2.3	n/a		
15.3.1	Eisen voor audits en andere activiteiten waarbij controles worden uitgevoerd op productiesystemen, behoren zorgvuldig te worden gepland en goedgekeurd om het risico van verstoring van	Covered by ISO 27001:2013 only	12.7.1	n/a	12.7.1	n/a		

BIR #	Control Description	Control Mapping	Office 365		Azure		Other documentation	Customer considerations
			ISO 27001: 2013	SOC 2	ISO 27001: 2013	SOC 2		
	bedrijfsprocessen tot een minimum te beperken.							
15.3.2	Toegang tot hulpmiddelen voor audits van informatie-systemen behoort te worden beschermd om mogelijke misbuik of compromittering te voorkomen.	Covered by FedRAMP only	n/a	n/a	n/a	n/a	Azure – FedRAMP: 13.3.9 Protection of Audit Information (AU-9)	

[1] Microsoft disclaimer	The report does not under any circumstance constitute a legally binding offer or acceptance of Microsoft Ireland Operations Limited or any other Microsoft Group affiliate. This report shall not be construed as (i) any commitment from Microsoft Ireland Operations Limited or any other Microsoft Group affiliate and/or (ii) supplementing or amending the terms of any existing agreement with Microsoft Ireland Operations Limited or any other Microsoft Group affiliate.

Appendix B - BIR

The Dutch government organizations should comply with the ISO 27001 / 27001 standard. This is covered in the Baseline Informatiebeveiliging Rijksdienst (BIR). The BIR provides one set of standards for the security of the information management of the central government. This makes it possible to work safely together and exchange data.

The BIR is entirely structured according to DIN / ISO 27001, Annex A and DIN / ISO 27002. Government organizations are obliged to comply with ISO 27001 and ISO 27002. The 'College Standaardisatie' has incorporated these requirements in the list of mandatory standards.

For more information regarding the BIR standard, please refer to:
http://www.earonline.nl/index.php/Overzicht_Baseline_Informatiebeveiliging_Rijksdienst_(BIR_2012)

Appendix C - Office 365 and Azure

Microsoft Office 365 and Azure are both cloud computing services provided by Microsoft. Microsoft Office 365 is a collection of services, which provides productivity software for subscribers. It encompasses Word, Excel, PowerPoint, Outlook, Publisher, ONEnote, Access, and Skype for Business. For more details, please refer to https://products.office.com/.

Microsoft Azure is a collection of cloud computing platform and infrastructure related services, enabling subscribers to build, deploy, and manage applications and services through a global network of Microsoft-managed data centers. For more details, please refer to https://azure.microsoft.com/.

Microsoft Office 365 is defined as Software-as-a-Service, whereas Microsoft Azure offers Platform-as-a-Service and Infrastructure-as-a-Service. Demonstrating control compliance to the BIR standard is different for both services, since the responsibility for the application layer in Microsoft Azure lays with the organization using the cloud services. This means Microsoft has no influence on how organizations implement the BIR controls in the application layer.

For more details regarding cloud computing, please refer to 'The NIST Definition of Cloud Computing' (Appendix D).

Appendix D - Documentation

The following table covers the documentation that was the basis of the coverage mapping for this analysis.

Document title	File name	Version
Compliance Framework for Industry Standards and Regulations	Compliance Framework document.pdf	May 2016
Azure ISO 27001:2013 – Audit Assessment Certificate	Azure and Power BI ISO 27001 Audit Assessment Certificate.pdf	21 Mar 2016
Azure ISO 27001:2013 – Statement of Applicability	Azure ISO Statement of Applicability SOA 2015 clickwraper protected.pdf	18 Feb 2016
Azure ISO 27001:2013 – Audit Report	Azure ISO 27001 Report Aug 2015_clickwraped-protected.pdf	28 Aug 2015 (8204184) 26 Aug 2015 (8364572)
Azure SOC 2 Type II – Audit Report	Azure SOC 2 AT 101 Type II Audit Report 2015	18 Nov 2015 (Signed) (15 Jan - 31 Jul 2015)
MCIO ISO 27001:2013 – Audit Assessment Certificate	MCIO ISO IEC 27001 2013 Certificate (IS 533913).pdf	21 Sep 2016
MCIO ISO 27001:2013 – Statement of Applicability	MCIO ISO Statement of Applicability SOA 2015 clickwraped-protected.pdf	18 Feb 2016
MCIO ISO 27001:2013 – Audit Report	MCIO ISO Audit Report -clickwraped-protected FY15.pdf	4 May 2015 (8129058)
MCIO SOC 2 Type II – Audit Report	MCIO AT 101 SOC 2 Type II Clickthrough Report 2015.pdf	2 Sep 2015 (Signed) (1 Oct 2014 - 30 Jun 2015)

Appendix D - Documentation (cont.)

Document title	File name	Version
Office 365 ISO 27001:2013 – Audit Assessment Certificate	Microsoft Office 365 ISO IEC 27001 2013 Certificate (IS 552878).pdf	21 Sep 2016
Office 365 ISO 27001:2013 – Statement of Applicability	Office 365 ISMS Statement of Applicability Security and Privacy.pdf	31 Oct 2014
Office 365 ISO 27001:2013 and ISO 27018:2014 – Audit Report	Office 365 ISO 27001 and ISO 27018 Audit Assessment Report 2015.pdf	26 Oct 2015 (8233538)
Office 365 SOC 2 Type II – Audit Report	Office 365 SOC 2 AT 101 Audit Report 2015.pdf	12 Oct 2015 (signed) (1 Oct 2014 - 30 Jun 2015)
Microsoft Online Service Terms	MicrosoftOnlineServicesTerms(English)(June2016)(CR).docx	1 Jun 2016
FedRAMP System Security Plan – Microsoft Azure	Azure FedRAMP System Security Plan SSP v2.3 protected.pdf	26 Feb 2016

The following table covers the additional documentation referred to in this report.

Document title	File name	Version
Data Resiliency in Office 365	Data Resiliency in Office 365.pdf	11 Feb 2016
The NIST Definition of Cloud Computing	nistspecialpublication800-145.pdf	Sep 2011

KPMG

KPMG on social media

Download on the App Store

KPMG app