



MICROSOFT AZURE, DYNAMICS 365 AND ONLINE SERVICES

ISO 27001:2013, ISO 27018:2019, ISO 27017:2015, AND ISO 27701:2019 SCOPE
EXPANSION REVIEW SUMMARY REPORT

DECEMBER 2, 2020

Attestation and Compliance Services



Proprietary & Confidential

Reproduction or distribution in whole or in part without prior written consent is strictly prohibited.

STATEMENT OF CONFIDENTIALITY

The sole purpose of this document is to provide Microsoft Corporation (Microsoft) with the summary of the ISO/IEC 27001:2013, ISO/IEC 27018:2019, ISO/IEC 27017:2015, and ISO/IEC 27701:2019 Scope Expansion review. At Microsoft's discretion, it may distribute this report to its clients. Each recipient of this report agrees that it shall not distribute or use the information contained herein and any other information regarding Microsoft for any purpose other than those stated. This document, and any other Microsoft related information provided, shall remain the sole property of Microsoft and may not be copied, reproduced, or distributed without the prior written consent of Microsoft.

APPLICABILITY

This document is supplemental to the ISO/IEC 27001:2013, ISO/IEC 27018:2019, ISO/IEC 27017:2015, and ISO/IEC 27701:2019 scope expansion review performed by Schellman & Company, LLC (Schellman), the primary deliverable which is the certificate. The information found in this report and the conclusions reached were dependent upon the complete and accurate disclosure of information by Microsoft. The information provided in this report is "AS IS" without warranties of any kind. Schellman expressly disclaims any warranties of representations including implied warranties and fitness for a particular purpose.

INDEPENDENCE DISCLOSURE

Schellman assessed the Information Security Management System (ISMS) and Privacy Information Management System (PIMS) for Microsoft. Schellman does not hold any investment or control over Microsoft. During the course of the assessment, Schellman did not willfully and unnecessarily market services to achieve conformance to ISO/IEC 27001:2013, ISO/IEC 27018:2019, ISO/IEC 27017:2015, and ISO/IEC 27701:2019. No Schellman service was recommended during the course of the engagement.

TABLE OF CONTENTS

SECTION 1 AUDIT TEAM RECOMMENDATION..... 1

SECTION 2 PROJECT OVERVIEW.....3

SECTION 3 SCOPE EXPANSION REVIEW
TESTING RESULTS 12

SECTION 4 CERTIFICATION CYCLE PROGRAM..... 16

APPENDIX A MICROSOFT AZURE SCOPE
STATEMENT20

SECTION I

AUDIT TEAM RECOMMENDATION

AUDIT TEAM RECOMMENDATION

Summary of Findings and Recommendation

Overall, the ISMS appears to be operating effectively and the client has met the requirements of the ISO/IEC 27001:2013 (ISO 27001) standard in addition to the control requirements included in the ISMS based on the control sets within the ISO/IEC 27017:2015 (ISO 27017) and ISO/IEC 27018:2019 (ISO 27018), and the privacy information management system (PIMS) processor requirements of ISO 27701:2019 (ISO 27701). There were no nonconformities noted during the October 2020 scope expansion review.

It is the audit team's recommendation to keep the certification in an active status and re-issue the certificate reflecting the updated ISMS scope.

Finding Ref	Status	Correction ¹	Corrective Action Plan ¹	Evidence of Remediation ¹
No nonconformities were identified during the 2020 scope expansion review.				

¹ Correction is the immediate action taken to address the nonconformance; the corrective action plan includes the root cause related to the nonconformance and the organization's plan to address the root cause; and evidence of remediation includes the implementation of the corrective action plan (i.e. the full implementation of the plan that addresses the root cause related to the nonconformance).

SECTION 2

PROJECT OVERVIEW

EXECUTIVE SUMMARY

Introduction

Microsoft Corporation (“Microsoft” or the “client”) underwent a scope expansion review in October 2020 of their ISO 27001:2013 (“ISO 27001” or the “standard”) certification which was originally issued in November 2011. The purpose of the scope expansion was to verify that the approved ISMS and PIMS continued to be in conformance with the ISO 27001, in addition to the management system requirements and control implementation guidance of ISO 27701 as well as the control implementation guidance within ISO 27017 and ISO 27018, as well as the internal policies and procedures based on the modifications to the ISMS scope. The scope expansion was relevant to the ISMS and PIMS and covered the addition of new offerings to the scope. This report includes the results of the 2020 scope expansion review mentioned above.

Schellman performed the scope expansion review to summarily review the documentation and maintenance, monitoring, and operating effectiveness of the ISMS and PIMS in order to achieve multiple objectives. The scope expansion review included the following:

- The ISMS maintenance elements which include the internal audit, measurement and monitoring, management review, and corrective action, as applicable to the scope expansion;
- Communications from external parties as required by the ISMS standard ISO 27001 and PIMS standard ISO 27701 and other documents required for certification, as applicable to the scope expansion;
- Changes to the documented system, as applicable to the scope expansion;
- Areas subject to change, as applicable to the scope expansion;
- Selected elements of ISO 27001, ISO 27017, ISO 27018, and ISO 27701, as applicable to the scope expansion; and
- Other selected areas as appropriate, as applicable to the scope expansion.

The scope of the scope expansion review was limited to the ISMS and PIMS modifications to include new offerings into the certified management system and review of unique processes. The full scope of the ISMS and PIMS is noted in Appendix A, which also includes the in-scope locations supporting the ISMS and PIMS.

Opening Meeting Description

An opening meeting occurred at approximately 10:00 AM PST on Thursday, Friday, October 16, 2020, remotely via conference call. A meeting agenda was provided as well as an audit plan for the scope expansion review.

The opening meeting was held to perform the following:

- Reconfirm the audit plan, scope, and deliverables for the review;
- Identify the client points of contact for the objectives and domains; and
- Discuss the timing expectations of the fieldwork as well as the activities following the fieldwork.

Audit Review Details

The scope expansion audit program included the following:

- Internal audits and management review;
- Effectiveness of the management system with regard to achieving the certified client's objectives;
- Progress of planned activities aimed at continual improvement;
- Continuing operational control;

- Review of any changes; and
- Use or marks and/or any reference to certification.

The scope expansion audit objectives included the following:

- Determine the continued conformance of the ISMS to the ISO 27001 standard and the PIMS to the ISO 27701 standard, specifically with regard to achieving the objectives of Microsoft's information security policy and Microsoft's maintenance, monitoring, and improvement activities of the ISMS and PIMS, specifically applicable to the scope expansion;
- Conformance to the PIMS requirements of ISO 27701; and
- Effectiveness of the procedures and processes for evaluation and review of compliance with relevant information security legislation and regulations, specifically applicable to the scope expansion.

During the assessment, all ISMS-related and PIMS-related documentation was available for the audit team to assess the ISMS and in relation to the audit objectives of this assessment.

The scope expansion review was conducted remotely and began on Monday, October 19, 2020, and ended on Wednesday, December 2, 2020, which included a closing, and included a discussion with the ISMS team regarding the scope expansion review results and the overall scope expansion review recommendation and next steps.

Confidentiality Statement

The information included in this report is to be treated as confidential.

OVERVIEW OF OPERATIONS

Company Background Description of Services Provided

Microsoft Azure is a cloud computing platform for building, deploying, and managing applications through a global network of Microsoft and third-party managed datacenters. It supports both Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud service models and enables hybrid solutions that integrate cloud services with customers' on-premises resources. Microsoft Azure supports many customers, partners, and government organizations that span across a broad range of products and services, geographies, and industries. Microsoft Azure is designed to meet their security, confidentiality, and compliance requirements.

Dynamics 365 is an online business application suite that integrates the Customer Relationship Management (CRM) capabilities and its extensions with the Enterprise Resource Planning (ERP) capabilities. Microsoft Dynamics 365 products/offerings and its supporting Datacenters are covered under the Azure, Dynamics 365, and Online Services report.

Microsoft datacenters support Microsoft Azure, Dynamics 365, and many other Microsoft Online Services ("Online Services"). Online Services such as Intune, Power BI, and others are Software as a Service (SaaS) services that leverage the underlying Microsoft Azure platform and datacenter infrastructure.

For a full description of the scope and services provided, refer to Appendix A.

ISMS AND PIMS REVIEW

General Design and Operating Effectiveness of the Client ISMS and PIMS

Microsoft Azure has effectively demonstrated that the additional services and offerings were incorporated into the scope of the ISMS and PIMS and included the requirements of ISO 27017, 27018 and the PIMS processor requirements of ISO 27701.

Microsoft Azure leadership, support, and commitment is demonstrated through ongoing monitoring activities, such as the risk assessments and management reviews, which have identified areas for management to address risk or improve the organization's risk posture. These plans were implemented through the support of planned resources made available by senior leadership, taking into consideration the needs and requirements of interested parties.

Clause	Conclusion	Comment
Context of the Organization	Effective	No Comment
Leadership – Commitment	Not Applicable	Note 1
Leadership – Policy	Not Applicable	Note 1
Leadership – Organizational Roles, Responsibilities, and Authorities	Not Applicable	Note 1
Planning – Risk Assessment	Effective	No Comment
Planning – Risk Treatment	Effective	No Comment
Planning – Objectives	Effective	No Comment
Support – Resources	Effective	No Comment
Support – Competence	Not Applicable	Note 1
Support – Awareness	Not Applicable	Note 1
Support – Communication	Not Applicable	Note 1
Support – Documentation	Effective	No Comment
Operation	Effective	No Comment
Performance Evaluation – Monitoring and Measurement	Effective	No Comment
Performance Evaluation – Internal Audit	Effective	No Comment
Performance Evaluation – Management Review	Effective	No Comment
Improvement – Nonconformity / Corrective Action	Not Applicable	Note 1
Improvement – Continual Improvement	Not Applicable	Note 1
Annex A Control Testing	Effective	No Comment
Annex A Control Testing and Additional ISO 27017, ISO 27018, and 27701 Implementation Guidance	Effective	No Comment

Clause	Conclusion	Comment
ISO 27017 Extended Control Set for Cloud Services Security	Effective	No Comment
ISO 27018 Extended Control Set for PII Protection	Effective	No Comment
ISO 27701 Annex B Control Testing for PII Processors	Effective	No Comment

Legend

Note 1 – Clause reference was assessed and found to be not impacted by the inclusion of the additional services and offerings into the scope of the ISMS and PIMS.

Context of the Organization (Clause 4)

Understanding the Organization and Its Context and the Needs and Expectations of Interested Parties (Clause 4.1 and 4.2)

Microsoft Azure has established an integrated management system (IMS) manual to provide an overview and the required specifics of the ISMS and PIMS for Microsoft Azure, Dynamics 365, and Online Services (Microsoft Azure). The ISMS manual includes the context of the organization, requirements of the interested parties, information security objectives, information security policy, ISMS relevant documentation, resources, security awareness and competence requirements, risk assessment and treatment, measurement, and monitoring requirements, internal audit plan and schedule, management review inputs and outputs as well as the corrective action and continual improvement processes.

Microsoft Azure has defined the internal and external interfaces and dependencies and their relationships that affect its ability to achieve the intended outcome(s) of its ISMS and PIMS.

The context of the organization, scope statement, interested parties, and internal and external issues were assessed during the scope expansion review and noted to be effectively implemented and in conformance with the requirements of the standard.

Determining the Scope of the ISMS (Clause 4.3)

The scope of the ISMS is defined and documented and most recently updated as of November 9, 2020. Note that the scope statement was updated after fieldwork, but prior to the closing meeting and drafting the report. It was noted that there were no material changes to the scope statement as it pertained to what was detailed in planning discussions with Microsoft prior to fieldwork. The scope of the ISMS is reviewed by the Microsoft Azure compliance manager at least annually or upon significant changes to internal and external interested parties.

The scope of the ISO 27001 scope expansion review was limited to the additional services and offerings being added to the ISMS and PIMS supporting Microsoft Azure, Dynamics 365, and other Online Services that were deployed in Azure Public, Government and Germany Cloud including their development, operations, and infrastructure and their associated security, privacy, and compliance and inclusive of the requirements and control implementation guidance of ISO 27701 for a PIMS as a data processor.

The scope of the ISMS and PIMS comprises the development, operations and infrastructure teams for Azure and Azure based services deployed in Public, Government and Germany Cloud, collectively referred as Microsoft Azure in accordance with the statement of applicability, version 2020.01, dated April 13, 2020.

The new offerings and services are within the scope and boundaries of the ISMS which consisted of Cloud Operations & Infrastructure (CO&I) fully managed datacenters, remotely managed datacenters, the core servers providing critical shared services and management tools for the infrastructure, and the access network infrastructure that supports these critical core services.

Information Security Management System (Clause 4.4)

The requirements of the ISMS and PIMS are well-defined throughout the ISMS manual with regards to continual improvement activities of the ISMS and PIMS. Microsoft Azure has established and continues to manage the ISMS in adherence to the ISO 27001, 27017, 27018 and 27701 standards and has aligned the ISMS with Microsoft Corporate policies and standards, as well as Microsoft Azure defined policies and standard operating procedures (SOPs).

Leadership, Organizational Structure, and Support (Clauses 5 and 7)

The requirements of Clauses 5 and 7 (Leadership, Organizational Structure, and Support) are well-defined in the ISMS Manual. The following aspects of the ISMS were tested during 2020 scope expansion review and were noted to be unchanged during the scope expansion review

- Leadership and Commitment (Clause 5.1)
- Policy (Clause 5.2)
- Organizational Roles, Responsibilities, and Authorities (Clause 5.3)
- Resources (Clause 7.1)
- Competence (Clause 7.2)
- Awareness (Clause 7.3)
- Communication (Clause 7.4)
- Documented Information (Clause 7.5)

Risk Identification, Risk Assessment, and Risk Treatment (Clauses 6 and 8)

Microsoft Azure's global risk management program (RMP) is in place to oversee and evaluate existing and emerging risks / threats to the Azure environment. The RMP aligns the risk management framework with the Microsoft Azure risk management procedures and processes (Azure engineering, service operation, infrastructure, and compliance).

Risk Assessment

Microsoft Azure has established a risk and exception SOP which documents the risk assessment process. Risk assessments are performed by global Azure services teams semi-annually to review the effectiveness of existing controls and safeguards, as well as to identify new risks. These assessments ensure all policies and supporting procedures properly address the environment considering changing regulatory, contractual, business, technical, and operational requirements.

A statement of applicability has been documented and lists the applicable controls from Annex A of ISO 27001, as well as any applicable ISO 27017, ISO 27018, and ISO 27701 controls that have been selected to mitigate risks as outlined in the risk assessment and risk treatment plan. It also details the controls that have been explicitly excluded with a justification for such exclusion. Per the statement of applicability, Microsoft does not outsource any development activities, and as a result, A.14.2.7 was justified for exclusion.

Schellman reviewed the risk assessment reports for a representative sample of services and offerings as part of scope expansion review and noted that the process for assessing risks was effective and in accordance with the requirements of the standard.

ISMS Effectiveness Measurements (Clause 9.1)

Microsoft Azure manages security key performance indicators (KPIs) to adequately measure security performance and effectiveness across the ISMS and PIMS. Annual, independent entity managed assessments are conducted

over the design and operating effectiveness of the control environment, which allow for the monitoring, measurement, analysis and evaluation of the controls. Monitoring is embedded in each service area supporting the ISMS and PIMS.

The monitoring, measurement, analysis, and evaluation process was noted to have been effectively implemented related to the additional services and offerings in accordance with the requirements of the standard.

Internal ISMS Audits (Clause 9.2)

Microsoft Azure management is committed to performing continuous independent reviews and assessments of its ISMS, PIMS, and control environment to ensure design and operating effectiveness of the controls is assessed and validated on periodic basis.

An independent internal audit was conducted surrounding the additional services and offerings as it pertained to the ISMS framework and applicable controls (including the ISO 27701 processor control activities). The results of ISMS internal audit activities were communicated to the relevant interested parties and the results were reviewed by members of ISMS management.

The internal audit efforts supporting the additional services and offerings was completed in October 2020 and was noted to be effectively implemented in accordance with the requirements of the standard.

Management Reviews (Clause 9.3)

Per the ISMS manual, leadership reviews are conducted to discuss progress, monitor changes, and provide input to the continuous improvement of information security and privacy KPIs relevant to the ISMS and PIMS. The leadership review of security and privacy goals and objectives addresses internal / external topics related to monitoring, trend analysis and issue mitigation and ensures the continuing suitability, adequacy, and effectiveness of ISMS. The inputs and outputs to ISMS management review along with the different types of reviews and their cadence are defined in the ISMS manual.

Schellman reviewed the evidence and determined that the management review process incorporated the considerations of the additional services and offerings and was effectively implemented in accordance with the requirements of the standard.

Corrective Action and Continual Improvement (Clause 10)

The requirements of Clause 10 (corrective action and continual improvement) were well-defined in the ISMS manual. As the new offerings and services were already incorporated as a part of Microsoft Azure, the following aspects of the ISMS were unaffected by the scope expansion review:

- Nonconformity and Corrective Action (Clause 10.1)
- Continual Improvement (Clause 10.2)

Additional Guidance for PII Processors (ISO 27701 Clause 8)

The following control areas of the PIMS were tested during 2020 scope expansion review and were noted to be unchanged during the scope expansion review:

- Customer Agreement (8.2.1)
- Organization's Purposes (8.2.2)
- Marketing and Advertising Use (8.2.3)
- Infringing Instruction (8.2.4)

- Customer Obligations (8.2.5)
- Obligations to PII Principals (8.3.1)
- Temporary Files (8.4.1)
- Return, Transfer or Disposal of PII (8.4.2)
- Basis for PII Transfer Between Jurisdictions (8.5.1)
- Countries and International Organizations to Which PII Can Be Transferred (8.5.2)
- Records of PII Disclosures to Third Parties (8.5.3)
- Notification of PII Disclosure Requests (8.5.4)
- Legally Binding PII Disclosures (8.5.5)
- Disclosure of Subcontractors Used to Process PII (8.5.6)
- Engagement of Subcontractors to Process PII (8.5.7)
- Change of Subcontractor to Process PII (8.5.8)

Conditions for Collection and Processing (8.2)

Records Related to Processing PII (8.2.6)

Microsoft maintains records in support of demonstrating compliance with its obligations for the processing of PII carried out on behalf of a customer. Specifically, an example Data Protection Impact Assessment for Microsoft's Infrastructure as a Service details how Microsoft processes data on behalf of customers and the technical and organizational measures in place to safeguard PII. Microsoft also makes available independent audit reports to its customers to help demonstrate compliance and the processing performed.

Privacy By Design and Privacy By Default (8.4)

PII Transmission Controls (8.4.3)

Microsoft Azure secures data transmitted over a data-transmission network via controls designed to ensure that the data reaches its intended destination. Microsoft Azure data in transit is encrypted via https. In addition, *How Azure Can Help Organizations Become GDPR Compliant* explains that Azure customers may implement a site-to-site VPN, to "create a virtual private connection between your on-premises network and an Azure Virtual Network."

Control Activities Supporting the ISMS and PIMS

Process walkthroughs were performed for the following Annex A control domains and the applicable controls from ISO 27017, ISO 27018, and ISO 27701 as they were determined to be impacted by the additional services and offerings relevant to the ISMS and PIMS:

- Logical Access
- Operations Security
- Communications Security
- Application Development
- Incident Management
- Business Continuity
- ISO 27017 extended control set for cloud services security
- ISO 27018 extended control set for PII protection
- ISO 27701 Annex B control testing for PII processors

The walkthroughs were performed with process and control owners during the project fieldwork.

FINDINGS OF NONCONFORMITY

Description of Findings (Major and Minor Nonconformities and Opportunities for Improvement)

There were no nonconformities noted as a result of the 2020 scope expansion review.

Explanation of ISO Requirement Classifications

This report provides management with identification of the documentation efforts, in addition to the review and testing of the maintenance, monitoring, and operating effectiveness of the ISMS in relation to the ISO 27001 standard requirements, specifically Clauses 4 through 10, the ISO 27701 standard requirements, and the control activities identified within Annex A, ISO 27017, ISO 27018 and ISO 27701 that are applicable to the ISMS. Documentation requirements as well as the maintenance, monitoring, and operating effectiveness of the ISMS have been classified according to their significance in achieving conformance to the standard. The classifications are defined as follows:

- **Conform (C)** – Based on observations, discussions with personnel, and inspection testing, these documentation requirements and/or controls are currently in place and found to be operating effectively.
- **Nonconformities (Major (MJ) and Minor (MN))**

Per definition from ISO 17021-1, a nonconformity is a nonfulfillment of the requirement. Major and Minor Nonconformity definitions are included below:

- **Major: nonconformity that affects the capability of the management system to achieve the intended results**
Note 1 to entry: Nonconformities could be classified as major in the following circumstances: 1) if there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements, or 2) a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity.
- **Minor: nonconformity that does not affect the capability of the management system to achieve the intended results**

- **Not Applicable (NA)** – The Clause was not applicable to the review.

SECTION 3

SCOPE EXPANSION REVIEW TESTING RESULTS

SCOPE EXPANSION REVIEW TESTING RESULTS

Note that requirements in the matrices below denoted with a caret (^) were noted as those requirements that included additional implementation requirements applicable to ISO 27701.

Clause	Subject Audited	Clause Classification				Remarks
		C	MN	MJ	NA	
ISO 27001 ISMS Clause Requirements						
4.1	Understanding the organization and its context	✓				
4.2	Understanding the needs and expectations of interested parties	✓				
4.3	Determining the scope of the information security management system	✓				
4.4	Information security management system	✓				
5.1	Leadership and commitment				✓	Note 1
5.2	Policy				✓	Note 1
5.3	Organizational roles, responsibilities, and authorities				✓	Note 1
6.1.1	General Planning	✓				
6.1.2	Information security risk assessment	✓				
6.1.3	Information security risk treatment	✓				
6.2	Information security objectives and planning to achieve them	✓				
7.1	Resources				✓	Note 1
7.2	Competence				✓	Note 1
7.3	Awareness				✓	Note 1
7.4	Communications				✓	Note 1
7.5.1	Documented information – general				✓	Note 1
7.5.2	Documented information – creating and updating				✓	Note 1
7.5.3	Control of documented information				✓	Note 1
8.1	Operational planning and control	✓				
8.2	Information security risk assessment	✓				
8.3	Information security risk treatment	✓				
9.1	Monitoring, measurement, analysis, and evaluation	✓				
9.2	Internal audit	✓				
9.3	Management review	✓				

Clause	Subject Audited	Clause Classification				Remarks
		C	MN	MJ	NA	
10.1	Nonconformity and corrective action				✓	Note 1
10.2	Continual improvement				✓	Note 1
ISO 27001 Annex A Control Objectives						
A.5^#	Information security policies				✓	Note 1
A.6^#	Organization of information security				✓	Note 1
A.7^#	Human resource security				✓	Note 1
A.8^#	Asset management				✓	Note 1
A.9^#	Access control	✓				
A.10^#	Cryptography				✓	Note 1
A.11^#	Physical and environmental security				✓	Note 1
A.12^#	Operations security	✓				
A.13^#	Communications security	✓				
A.14^#	Systems acquisition, development, and maintenance	✓				
A.15^#	Supplier relationships				✓	Note 1
A.16^#	Information security incident management				✓	Note 1
A.17	Information security aspects of business continuity management	✓				
A.18^#	Compliance				✓	Note 1
ISO 27017 Extended Control Set for Cloud Services Security						
CLD.6.3	Relationship Between Cloud Service Customer and Cloud Service Provider				✓	Note 1
CLD.8.1	Responsibility for Assets				✓	Note 1
CLD.9.5	Access Control of Cloud Service Customer Data in Shared Virtual Environment	✓				
CLD.12.1	Operational Procedures and Responsibilities	✓				
CLD.12.4	Logging and Monitoring	✓				
CLD.13.1	Network Security Management	✓				
ISO 27018 Extended Control Set for PII Protection						
A.2	Consent and Choice				✓	Note 1
A.3	Purpose legitimacy and specification				✓	Note 1
A.5	Data minimization	✓				
A.6	Use, retention, and disclosure				✓	Note 1
A.8	Openness, transparency, and notice				✓	Note 1

Clause	Subject Audited	Clause Classification				Remarks
		C	MN	MJ	NA	
A.10	Accountability	✓				
A.11	Information security	✓				
A.12	Privacy compliance	✓				
ISO 27701 PIMS Clause Requirements						
5.2	Context of the organization	✓				
5.4	Planning	✓				
ISO 27701 Annex B Extended Control Set for PII Processors						
B.8.2	Conditions for Collection and Processing	✓				
B.8.3	Obligations to PII Principals				✓	Note 1
B.8.4	Privacy by Design and Privacy Default	✓				
B.8.5	PII Sharing, Transfer and Disclosure				✓	Note 1

Legend

Note 1 – Clause reference was assessed and found to be not impacted by the inclusion of the additional services and offerings into the scope of the ISMS and PIMS.

Note that controls in the above matrices denoted with a carat key (^) and/or asterisk (*) and/or pound (#) were noted as those controls that included additional guidance, and subsequent testing, applicable to supplemental control guidance from ISO 27017 (^), 27018 (*), and 27701 (#), respectively.

SECTION 4

CERTIFICATION CYCLE PROGRAM

SURVEILLANCE REVIEW SCHEDULE

Year	Type of Review	Processes to be Assessed	Locations to be Assessed	Planned / Applied Audit Time	Dates
2020	Recertification	ISMS / PIMS framework and full system scope, including ISO 27017, 27018 and 27701	Redmond, WA Sampled Data Centers	14 days remote auditing / 2 days planning and reporting	March – April 2020
2020	Scope Expansion	<ul style="list-style-type: none"> ISMS / PIMS Framework Annex A <ul style="list-style-type: none"> Access control Operations security Communications security System development Business continuity ISO 27017 control implementation guidance ISO 27018 control implementation guidance ISO 27701 processor control implementation guidance 	Redmond, WA	14 days remote auditing / 2 days planning and reporting	October 2020

Year	Type of Review	Processes to be Assessed	Locations to be Assessed	Planned / Applied Audit Time	Dates
2021	Surveillance	<ul style="list-style-type: none"> ISMS / PIMS Framework Information security policy Organization of Information Cryptography Physical and environmental security System development Supplier relationship Business continuity management Compliance ISO 27017 cloud implementation guidance for the applicable Annex A controls ISO 27018 cloud implementation guidance for the applicable Annex A controls ISO 27701 processor control implementation guidance 	Redmond, WA Sampled Data Centers	7 days auditing / 2.5 days planning and reporting	March 2021
2022	Surveillance	<ul style="list-style-type: none"> ISMS / PIMS Framework Human resources security Asset management Access control Physical and environmental security Operations security Communications security Security incident management ISO 27017 cloud implementation guidance for the applicable Annex A controls ISO 27018 cloud implementation guidance for the applicable Annex A controls ISO 27018-specific Annex (A2 – A12) ISO 27701 processor control implementation guidance 	Redmond, WA Sampled Data Centers	7 days auditing / 2.5 days planning and reporting	March 2022

Year	Type of Review	Processes to be Assessed	Locations to be Assessed	Planned / Applied Audit Time	Dates
2023	Recertification	ISMS / PIMS framework and full system scope, including ISO 27017, 27018 and 27701 processor control implementation guidance	Redmond, WA Sampled Data Centers	13.5 days auditing / 5.5 days planning and reporting	March – April 2023

☐ Future projects

APPENDIX A

MICROSOFT AZURE SCOPE STATEMENT

MICROSOFT AZURE SCOPE STATEMENT

Scope of the ISMS and PIMS

The scope of the integrated management system (IMS) includes the ISMS, PIMS, SMS, BCMS, and QMS the development, operations and infrastructure teams for Azure and Azure based services deployed in Public, Government and Germany Cloud, collectively referred as Microsoft: Azure, Dynamics 365, and other Online Services in accordance with its IMS Statement of Applicability.

Microsoft: Azure, Dynamics 365, and other Online Services IMS applies to information resources, processes, and personnel within the Microsoft: Azure, Dynamics 365, and other Online Services Group. Information Resources include any Microsoft: Azure, Dynamics 365, and other Online Services owned or managed systems, applications, and network elements, and any information processed by, or used to provide Microsoft services. The scope of the ISMS includes the control requirements of ISO/IEC 27017:2015 and ISO/IEC 27018:2019 and the management system and control requirements of ISO/IEC 27701:2019 for PII processors.

Azure Cloud-Based Services Inclusions

Product Category	Service / Offering Name	Cloud Environment Scope		
		Azure	Azure Government	Azure Germany
Microsoft Azure Services				
AI + Machine Learning	Azure Bot Service	✓	✓	-
	Azure Open Datasets	✓	-	-
	Cognitive Services	✓	✓	-
	Cognitive Services: Form Recognizer	✓	-	-
	Cognitive Services: Computer Vision	✓	✓	-
	Cognitive Services: Container Platform	✓	-	-
	Cognitive Services: Content Moderator	✓	✓	-
	Cognitive Services: Custom Vision	✓	✓	-
	Cognitive Services: Custom Decision Service	✓	-	-
	Cognitive Services: Cognitive Service Platform	✓	✓	-
	Cognitive Services: Face	✓	✓	-
	Cognitive Services: Text Analytics	✓	✓	-
	Cognitive Services: Language Understanding	✓	✓	-
	Cognitive Services: Translator Text	✓	✓	-
	Cognitive Services: QnAMaker	✓	✓	-
	Cognitive Services: Speech Services	✓	✓	-
	Cognitive Services: Video Indexer	✓	-	-
	Machine Learning Service	✓	✓	-
	AI Builder	✓	✓	✓

Product Category	Service / Offering Name	Cloud Environment Scope		
		Azure	Azure Government	Azure Germany
	Machine Learning Studio	✓	-	✓
	Microsoft Genomics	✓	-	-
	Enterprise Knowledge Graph	✓	-	-
Analytics	Azure Analysis Services	✓	✓	✓
	Azure Data Explorer	✓	✓	✓
	Azure Synapse Analytics (formerly - SQL Data Warehouse)	✓	✓	✓
	Data Factory	✓	✓	✓
	HDInsight	✓	✓	✓
	Stream Analytics	✓	✓	✓
	Data Catalog	✓	✓	✓
	Data Lake Analytics	✓	-	-
	Azure Data Share	✓	-	-
	Azure Data Lake Storage Gen1	✓	✓	-
	Desktop Analytics	✓		
Compute	Cloud Services	✓	✓	✓
	Service Fabric	✓	✓	✓
	Virtual Machine Scale Sets	✓	✓	✓
	Virtual Machines (including SQL VM)	✓	✓	✓
	Batch	✓	✓	✓
	Functions	✓	✓	✓
	App Services <ul style="list-style-type: none"> App Service - Web Apps (including Containers) App Service – Application Program Interface (API) Apps App Service - Mobile Apps 	✓	✓	✓
	Azure App Service Static Web Apps	✓	✓	✓
	Guest Configuration	✓	✓	-
	Azure VMware Solution	✓	-	-
	Azure Kubernetes Configuration Management	✓		
	Planned Maintenance	✓	✓	✓
	Azure Spring Cloud	✓		
	Azure Arc enabled Servers	✓		
	Azure Arc enabled Kubernetes	✓		

Product Category	Service / Offering Name	Cloud Environment Scope		
		Azure	Azure Government	Azure Germany
	Azure VM Image Builder	✓		
Containers	Azure Kubernetes Service (AKS)	✓	✓	-
	Azure Red Hat OpenShift (ARO)	✓	-	-
	Container Instances	✓	✓	-
	Container Registry	✓	✓	-
	Azure Container Service	✓	✓	-
Databases	Azure Cosmos DB	✓	✓	✓
	Azure SQL Database	✓	✓	✓
	Azure Database for MariaDB	✓	✓	-
	Azure Database for MySQL	✓	✓	-
	Azure Database for PostgreSQL	✓	✓	-
	Azure Database Migration Service	✓	✓	-
	Azure Cache for Redis (including Premium)	✓	✓	✓
	Azure API for FHIR	✓	-	-
	SQL Server Registry	✓		
Developer Tools	Azure DevTest Labs	✓	✓	-
	Azure Lab Services	✓	✓	-
	Azure for Education	✓	-	-
	Application Change Analysis	✓	-	-
	Azure App Configuration	✓	-	-
Identity	Azure Information Protection	✓	✓	-
	Azure Active Directory (Free, Basic, Premium)	✓	✓	✓
	Microsoft Accounts	✓	-	-
	Azure Active Directory B2C	✓	-	-
	Azure Active Directory Domain Services	✓	✓	-
Integration	Service Bus	✓	✓	✓
Internet of Things	Event Hubs	✓	✓	✓
	Event Grid	✓	✓	-
	IoT Central	✓	-	-
	IoT Hub	✓	✓	✓
	Azure Maps	✓	✓	-
	Notification Hubs	✓	✓	✓
	Time Series Insights	✓	-	-

Product Category	Service / Offering Name	Cloud Environment Scope		
		Azure	Azure Government	Azure Germany
	Windows 10 IoT Core Services	✓	-	-
	Logic Apps	✓	✓	-
	API Management	✓	✓	✓
	Microsoft Azure Peering Service	✓	-	-
Management and Governance	Azure Resource Manager	✓	✓	✓
	Automation	✓	✓	-
	Azure Advisor	✓	✓	-
	Azure Lighthouse	✓	✓	-
	Azure Managed Applications	✓	✓	-
	Azure Migrate	✓	✓	-
	Azure Monitor	✓	✓	-
	Azure Policy	✓	✓	-
	Azure Resource Graph	✓	✓	-
	Cloud Shell	✓	✓	-
	Microsoft Azure Portal	✓	✓	✓
	Azure Blueprints	✓	-	-
	Nomination Portal	✓	✓	
	Scheduler	✓	✓	✓
	Cost Management	✓	✓	-
	Azure Performance Diagnostics	✓	-	-
Media	Media Services	✓	✓	✓
Mixed Reality	Azure Spatial Anchors	✓	-	-
	Azure Remote Rendering	✓		
Networking	Application Gateway	✓	✓	✓
	Azure Load Balancer	✓	✓	✓
	ExpressRoute	✓	✓	✓
	Virtual Network	✓	✓	✓
	VPN Gateway	✓	✓	✓
	Azure Bastion	✓	✓	✓
	Azure DDoS Protection	✓	✓	-
	Azure DNS	✓	✓	✓
	Azure Firewall	✓	✓	-
	Azure Firewall Manager	✓	-	-

Product Category	Service / Offering Name	Cloud Environment Scope		
		Azure	Azure Government	Azure Germany
	Azure Front Door	✓	✓	-
	Azure Internet Analyzer	✓	-	-
	Azure Private Link	✓	✓	-
	Azure Web Application Firewall	✓	✓	-
	Content Delivery Network	✓	-	-
	Network Watcher	✓	✓	✓
	Traffic Manager	✓	✓	✓
	Virtual WAN	✓	✓	-
	Azure Public IP	✓	✓	✓
	Virtual Network NAT	✓	✓	-
Security	Key Vault	✓	✓	✓
	Azure Advanced Threat Protection	✓	✓	-
	Multi-Factor Authentication	✓	✓	✓
	Azure Dedicated HSM	✓	✓	-
	Azure LockBox	✓	-	-
	Azure Sentinel	✓	✓	-
	Security Center	✓	✓	-
	Azure Sphere	✓	-	-
	Microsoft Azure Attestation	✓		
	Azure Confidential Computing Offering for PCK Cache Service	✓		
	Azure Security Center for IoT	✓		
	Azure Security for IoT	✓	-	-
Storage	Storage (Blobs (including Azure Data Lake Storage Gen 2), Disks, Files, Queues, Tables) including Cool and Premium	✓	✓	✓
	Archive Storage	✓	✓	-
	Azure Import/Export	✓	✓	-
	Azure Data Box	✓	✓	-
	Azure HPC Cache	✓	-	-
	Site Recovery	✓	✓	✓
	StorSimple	✓	✓	-
	Backup	✓	✓	✓
	Azure NetApp Files	✓	✓	

Product Category	Service / Offering Name	Cloud Environment Scope		
		Azure	Azure Government	Azure Germany
	Lustre as a Service	✓	-	-
Web	Azure Search	✓	✓	-
	Azure SignalR Service	✓	-	-
Windows Virtual Desktop	Windows Virtual Desktop	✓	-	-
Supporting Infrastructure and Platform Services		✓	✓	✓

Microsoft Online Services			
Service/Offering Name	Public	US Government	Germany
Intune	✓	✓	-
Microsoft Cloud App Security	✓	✓	-
Microsoft Graph	✓	✓	✓
Microsoft Managed Desktop	✓	-	-
Microsoft Stream	✓	✓	-
Power Apps	✓	✓	-
Power Automate (Formerly Microsoft Flow)	✓	✓	-
Power BI	✓	✓	✓
Power BI Embedded	✓	✓	✓
Power Virtual Agents	✓	-	-
Microsoft Threat Experts	✓	-	-
Microsoft Defender for Endpoint (Formerly called Microsoft Defender Advanced Threat Protection)	✓	✓	-
Microsoft 365 Defender	✓	✓	
Microsoft Healthcare Bot	✓	-	-
Microsoft Bing for Commerce	✓		
Universal Print	✓		

Microsoft Dynamics 365			
Service/Offering Name	Public	US Government	Germany
Dynamics 365 Customer Engagement	✓	✓	✓
Dynamics 365 Customer Service	✓	✓	-
Dynamics 365 Customer Service Insights	✓	-	-

Microsoft Dynamics 365			
Service/Offering Name	Public	US Government	Germany
Dynamics 365 Customer Insights engagement insights	✓		
Dynamics 365 Field Service	✓	✓	-
Dynamics 365 Sales	✓	✓	✓
Dynamics 365 Sales Professional	✓		
Dynamics 365 Sales Insights	✓		
Dynamics 365 AI Customer Insights	✓	-	-
Dynamics 365 Business Central	✓	-	-
Dynamics 365 Finance	✓	-	-
Dynamics 365 Fraud Protection	✓	-	-
Dynamics 365 Marketing	✓	-	-
Dynamics 365 Portals	✓	✓	✓
Dynamics 365 Project Service Automation	✓	-	-
Dynamics 365 Project Operations	✓		
Dynamics 365 Retail	✓	-	-
Dynamics 365 Supply Chain Management	✓	-	-
Dynamics 365 Commerce	✓	-	-
Dynamics 365 Human Resources	✓	-	-
Chat for Dynamics 365	✓	✓	-
Dynamics 365 Athena - CDS to Azure Data Lake	✓	-	-
Dynamics 365 Guides	✓	✓	
Dynamics 365 Remote Assist	✓	✓	

Physical Environment

Microsoft: Azure, Dynamics 365, and other Online Services are hosted in datacenters located throughout the world, which are managed by Azure's Physical Infrastructure team. The Physical Infrastructure team provides the physical and logical infrastructure for Microsoft's cloud and hosted applications. The Physical Infrastructure team serves as the underlying platform that supports Microsoft's software plus service strategy. The physical infrastructure includes the datacenter facilities, as well as the hardware and software components that support the services and networks. At Microsoft, the logical infrastructure consists of operating system instances, routed networks, and unstructured data storage, whether running on virtual or physical assets. Platform services include compute runtimes, identity, and directory stores (such as Active Directory® and Microsoft account), and other advanced functions consumed by Microsoft properties.

Locations Covered by this Report

Azure production infrastructure is located in globally distributed datacenters. These datacenters deliver the core physical infrastructure that includes physical hardware asset management, security, data protection, networking

services. These datacenters are managed, monitored, and operated by Microsoft operations staff delivering online services with 24x7 continuity. The purpose-built facilities are part of a network of datacenters that provide mission critical services to Azure and other Online Services. The locations and datacenters within the scope of IMS are:

Main Location of the ISMS	
Redmond, Washington	One Microsoft Way Redmond, Washington 98052 United States

Microsoft Azure Domestic Datacenters	
West US	Santa Clara, CA (BY3/4/5/21/22/24/30) San Jose, CA (SJC20/21/31)
West US 2	Quincy, WA (CO1/2/6, MWH01/02/03/04/05)
West Central US	Cheyenne, WY (CYS01/04/05)
Central US	Des Moines, IA (DM1/2/3, DSM05/06/07/08)
North Central US	Chicago, IL (CH1/3/4, CHI20/21)
South Central US	San Antonio, TX (SN1/2/3/4/6/7, SAT09/10/20)
East US	Bristow, VA (BLU) Reston, VA (BL4/31) Sterling, VA (BL20) Ashburn, VA (BL2/3/5/6/7/21/22/23/30) Manassas, VA (MNZ20)
East US 2	Boydton, VA (BN1/3/4/6/7/8/9/10/13/14)
US GOV Iowa	Des Moines, IA (DM2)
US GOV Arizona	Phoenix, AZ (PHX20/21)
US GOV Texas	San Antonio, TX (SN5)
US GOV Virginia	Boydton, VA (BN1/11/12)

Microsoft Azure International Datacenters	
Canada East	Quebec, Canada (YQB20)
Canada Central	Toronto, Canada (YTO20/21/22/23)
Brazil South	Campinas, Brazil (CPQ01/02/20/22/24) Sao Paulo, Brazil (GRU)
Brazil Southeast	Rio de Janeiro, Brazil (RIO01/20)
West Europe	Amsterdam, Netherlands (AM1/2/3, AMS04/05/06/07/08/20/21/22/23)
North Europe	Dublin, Ireland (DB3/4/5, DUB06/07/08/09/12/20/21/24)
UK South	London, United Kingdom (LON21/22/23/24)
UK West	Cardiff, United Kingdom (CWL20)
France Central	Paris, France (PAR20/21/22/23)
France South	Marseille, France (MRS20)

Microsoft Azure International Datacenters	
Germany North	Berlin, Germany (BER20)
Germany Northeast	Leipzig-Halle, Germany (LEJ20)
Germany West Central	Frankfurt, Germany (FRA21/22/23)
Germany Central	Frankfurt (FRA20)
Switzerland West	Geneva, Switzerland (GVA20)
Switzerland North	Zurich, Switzerland (ZRH20)
East Asia	Hong Kong (HK2, HKG20/21)
Southeast Asia	Singapore (SG2/3, SIN20/21/22)
Southeast Asia 2	Cyberjaya, Malaysia (KUL01)
West India	Mumbai, India (BOM01)
Central India	Dighi, India (PNQ01/20/21)
South India	Ambattur, India (MAA01)
Japan West	Osaka, Japan (OSA01/02/20/21/22)
Japan East	Tokyo, Japan (TYO01/20/21/22/31)
Korea South	Busan, South Korea (PUS20)
Korea Central	Seoul, South Korea (SEL20/21)
UAE Central	Abu Dhabi (AUH20)
UAE North	Dubai (DXB20/21)
Australia East	Macquarie Park, Australia (SYD03) Sydney, Australia (SYD21/22/23/25/26/27)
Australia Southeast	Melbourne, Australia (MEL01/20/21/23)
Australia Central	Canberra, Australia (CBR20/22)
Australia Central 2	Canberra, Australia (CBR21)
South Africa North	Johannesburg, South Africa (JNB20/21/22)
South Africa West	Cape Town, South Africa (CPT20)
Norway East	Oslo, Norway (OSL20)
Norway West	Stavanger, Norway (SVG20)

Additional Microsoft Online Services Datacenters	
Southeast Asia 2	Cyberjaya, Malaysia (KUL01)
Korea South 2	Busan, South Korea (PUS01)
Brazil Northeast	Fortaleza, Brazil (FOR01)
Chile Central	Santiago, Chile (SCL01)
East Europe	Vienna, Austria (VIE)
North Europe 2	Vantaa, Finland (HEL01)

Edge Sites	
Ashburn, VA (ASH)	Manila, Philippines (MNL30)
Athens, Greece (ATH01)	Marseille, France (MRS01)
Atlanta, GA (ATA)	Minneapolis, MN (MSP30)
Auckland, New Zealand (AKL01/30)	Miami, FL (MIA)
Bangkok, Thailand (BKK30)	Milan, Italy (MIL30)
Barcelona, Spain (BCN30)	Montreal, Canada (YMQ01)
Berlin, Germany (BER30)	Moscow Russia (MOW30)
Bogota, Columbia (BOG30)	Mumbai, India (BOM02)
Boston, MA (BOS01/31)	Munich, Germany (MUC30)
Brisbane, Australia (BNE01)	Nairobi, Kenya (NBO30)
Brussels, Belgium (BRU30)	New Delhi, India (DEL01)
Bucharest, Romania (BUH01)	New York City, NY (NYC)
Budapest, Hungary (BUD01)	Newark, NJ (EWR30)
Buenos Aires, Argentina (BUE30)	Osaka, Japan (OSA30/31)
Busan, South Korea (PUS03)	Oslo, Norway (OSL30)
Cape Town, South Africa (CPT02)	Palo Alto, CA (PAO)
Chennai, India (MAA02)	Paris, France (PAR02/PRA)
Chicago, IL (CHG)	Perth, Australia (PER01/30)
Copenhagen, Denmark (CPH30)	Phoenix, AZ (PHX01/31)
Dallas, TX (DAL, DFW30)	Portland, OR (PDX31)
Denver, CO (DEN02, DNA)	Prague, Czech Republic (PRG01)
Detroit, MI (DTT30)	Puerto Rico (PR1)
Dubai, United Arab Emirates (DXB30)	Queretaro, Mexico (MEX30)
Frankfurt, Germany (FRA/FRA31)	Rome, Italy (ROM30)
Geneva, Switzerland (GVA30)	Sao Paulo, Brazil (SAO03)
Helsinki, Finland (HEL03)	San Jose, CA (SJC)
Ho Chi Minh, Vietnam (SGN30)	Santiago, Chile (SCL30)
Hong Kong (HKB)	Seattle, WA (STB)
Honolulu, HI (HNL01)	Seoul, South Korea (SLA)
Houston, TX (HOU01)	Singapore (SGE, SG1, SIN30)
Hyderabad, India (HYD30)	Sofia, Bulgaria (SOF01)
Istanbul, Turkey (IST30)	Stockholm, Sweden (STO)
Jakarta, Indonesia (JKT30)	Taipei, Taiwan (TPE30/31)
Johannesburg, South Africa (JNB02)	Tel Aviv, Israel (TLV30)
Kuala Lumpur, Malaysia (KUL02/30)	Tokyo, Japan (TYA/TYB)
Las Vegas, NV (LAS01)	Toronto, Canada (YTO01)

Edge Sites	
Lisbon, Portugal (LIS01)	Vancouver, Canada (YVR01/30)
Los Angeles, CA (LAX)	Vienna, Austria (VIE)
Lagos, Nigeria (LOS30)	Warsaw, Poland (WAW01)
London, United Kingdom (LTS)	Zagreb, Croatia (ZAG30)
Madrid, Spain (MAD30)	Zurich, Switzerland (ZRH)
Manchester, United Kingdom (MAN30)	

In addition to datacenter, network, and personnel security practices, Azure also incorporates security practices at the application and platform layers to enhance security for application development and service administration.