MICROSOFT AZURE, DYNAMICS 365, AND ONLINE SERVICES

ISO/IEC 27001:2022, ISO 27018:2019, ISO 27017:2015, AND ISO 27701:2019 CERTIFICATION - SCOPE EXPANSION REVIEW SUMMARY REPORT

NOVEMBER 21, 2024

Assessment and Compliance Services

Statement of Confidentiality and Distribution List

The sole purpose of this document is to provide Microsoft Corporation (Microsoft) with the summary of the ISO/IEC 27001:2022 (ISO 27001), ISO/IEC 27018:2019 (ISO 27018), ISO/IEC 27017:2015 (ISO 27017), and ISO/IEC 27701:2019 (ISO 27701) 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 27001, ISO 27018, ISO 27017, and ISO 27701 scope expansion review performed by Schellman Compliance, 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 27001, ISO 27018, ISO 27017, or ISO 27701. No Schellman service was recommended during the course of the engagement.

TABLE OF CONTENTS

SECTION 1

AUDIT TEAM RECOMMENDATION AND AUDIT RESULTS

Audit Team Recommendation, Audit Findings, and General Design and Operating Effectiveness of the ISMS and PIMS

Summary of Findings and Recommendation, General Design and Operating Effectiveness of the Client ISMS and PIMS

Overall, the ISMS appears to be operating effectively and the client has met the requirements of the ISO 27001 standard, in addition to the control requirements included in the ISMS and based on the control sets within ISO 27017 and ISO 27018, and the PIMS requirements of ISO 27701 in the role of a data processor. Microsoft Azure has effectively demonstrated that the additional services and offerings were incorporated into the scope of the ISMS and PIMS. There were no nonconformities or opportunities for improvement (OFIs) noted as a result of the 2024 scope expansion review.

It is the audit team's recommendation to keep the certification in an active status and issue an updated certificate reflecting the updated ISMS and PIMS scope based on modifications made since the 2024 surveillance review.

The ISMS and PIMS have adapted and demonstrated maturity over time, with the support of senior leadership, who have provided resources necessary to maintain and implement risk treatment plans and project initiatives designed to improve the risk posture of the organization. Policies are well-defined, detailed, reviewed, and updated regularly, communicated, and understood by users within the organization. The policies and procedures are designed in accordance with the ISO 27001 standard in addition to the control requirements included in the ISMS based on the control sets within the ISO 27017 and ISO 27018, and the PIMS processor requirements of ISO 27701.

The ISMS and PIMS have demonstrated improvement through ongoing monitoring activities, such as the risk assessments and management reviews, which have identified areas for management to address risk or improve the company's risk posture via implementation of new security programs and initiatives, the addition of security and compliance personnel to ensure that the ISMS and PIMS operate as intended, and implementation of new security tools and processes designed to manage risk, both manual and automated. 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, and driven by external and internal factors such as organizational changes, new business opportunities, updates to regulation and legislation, and newly identified security risks.

Finding Ref	Status	Corrective Action Plan[1]	Evidence of Correction[1]	Evidence of Remediation[1]
No nonconformities were identified during the 2024 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).

As part of the assessment, Schellman concluded that the scope of the ISMS and PIMS was appropriate, and the audit objectives of the scope expansion review were met.

Clause	Conclusion	Comment
Context of the Organization and additional ISO 27701 requirements	Effective	No Comment
Leadership	Not Applicable	Note 1
Planning and additional ISO 27701 requirements	Effective	No Comment
Support	Not Applicable	Note 1
Operation	Effective	No Comment
Performance Evaluation	Effective	No Comment
Improvement	Not Applicable	Note 1

Clause	Conclusion	Comment
Annex A Control Testing and Additional ISO 27017, ISO 27018, and 27701 Implementation Guidance	Effective	No Comment
ISO 27017 Extended Control Set for Cloud Services Security	Effective	No Comment
ISO 27018 Extended Control Set for Personal Identifiable Information (PII) Protection	Not Applicable	Note 1
ISO 27701 Annex B Control Testing for PII Processors	Effective	No Comment

Legend

Note 1 – Clause / Control Activity 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; therefore, with no change for the requirement or control relevant to the scope expansion, the testing Conclusion was deemed Not Applicable.

ISMS and PIMS Maintenance Activities

Microsoft Azure has updated relevant ISMS and PIMS documentation to reflect the addition of the following 36 service offerings to the scope of the ISMS, to be reflected on the updated ISO 27001 certificate:

- Azure Files
- Azure SQL Managed Instance
- Virtual Machines Licenses
- Microsoft Container Registry
- API Center
- Azure Arc-enabled VMware Solution
- Azure Business Continuity Center
- Azure Elastic SAN
- Azure Help
- Azure Modeling and Simulation Workbench
- Azure Stack
- Azure Update Manager
- Community Training
- Copilot for Service
- Dynamics 365 Contact Center
- Microsoft Global Secure Access
- Sustainability Data Services
- AFOI-Network Cloud
- Azure Confidential Ledger
- Azure Health AI Deidentification Service
- Azure Large Instance for Epic v1.1
- Microsoft Entra ID Governance
- Microsoft Security Copilot
- Arc User Experiences
- Azure Container Storage
- Defender EASM
- Dynamics 365 Human Resources (Operation)
- Dynamics 365 - Resource Scheduling Optimization
- Virtual Machine Extensions
- Nutanix on Azure
- Online Experimentation
- Publisher Verification Service and Application Consent Service
- Quota Management
- SaaS API
- Virtual Machines Bav2 Series
- Virtual Machines Bv2 Series

The aforementioned changes were noted to have been appropriately incorporated into the scope of the ISMS and PIMS and the supporting management system documentation.

Performance of the ISMS and PIMS Over the Certification Cycle

Overall, Microsoft continued to demonstrate a sound understanding of its ISMS and PIMS as it continued to meet the requirements of the ISO 27001 and ISO 27701 standards, in addition to the control requirements included in the ISMS and based on the control sets within ISO 27017, ISO 27018, and maintenance and operation of the PIMS based on the requirements and control implementation guidance of ISO 27701. The ISMS and PIMS and control framework are established, have been supported by top management, and are supported by a competent team dedicated to the foundation and maintenance of the management system. Microsoft continued to expand their ISMS scope to include additional service offerings and data center locations and did so in continued conformance of the ISO 27001 and ISO 27701 standards and 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.

Further, there have been no complaints and Microsoft has properly marketed their certificate in accordance with the client obligations and marketing guidelines provided to Microsoft. Lastly, as part of the ISMS and PIMS Microsoft has procedures in place to effectively monitor compliance with relevant information security and privacy legislation and regulations.

SECTION 2

PROJECT OVERVIEW

EXECUTIVE SUMMARY

Introduction

Microsoft (or the "client") underwent a scope expansion review in October 2024 of their ISO 27001 (or the "standard") certification which was originally issued in November 2011. The purpose of the scope expansion review was to verify that the approved ISMS and PIMS continued to be in conformance with the ISO 27001 standard, in addition to the management system requirements, control set, and control implementation guidance of ISO 27701, as well as the control set and control implementation guidance within ISO 27017 and ISO 27018, and internal policies and procedures based on the modifications to the ISMS and PIMS scope. The scope expansion relevant to the ISMS and PIMS covered the addition of 36 new offerings and one set of infrastructure services to the scope. This report includes the results of the 2024 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 and PIMS 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 incorporate additional services and offerings into the certified management system, and review of unique processes.

The scope of the ISMS and PIMS as a result of the scope expansion can be found in the Appendix.

Opening Meeting Description

An opening meeting occurred remotely utilizing the Microsoft Teams web conferencing application at approximately 10:00 AM PDT on Monday, September 9, 2024. An agenda was provided as well as a project plan and audit plan for scope expansion review. The opening meeting was held to perform the following:

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

Audit Review Details

The scope expansion audit covered the documentation requirements of the ISO 27001 and ISO 27701 standards and control guidance and sets of the ISO 27017 and ISO 27018 standards, as well as testing which included evidence of the monitoring, maintenance, and operating effectiveness of the ISMS and PIMS and testing of the applicable control framework.

The scope expansion audit objectives included the following:

- Determine the continued conformance of the ISMS and PIMS to the ISO 27001 and ISO 27701 standards, specifically with regard to achieving the objectives of Microsoft's policy and Microsoft's maintenance, monitoring, and improvement activities of the ISMS and PIMS, all relevant to the subject of the scope expansion.
- Effectiveness of the procedures and processes for evaluation and review of compliance with relevant information security legislation and regulations, all relevant to the subject of the scope expansion.
- Validate the functions at each in-scope location to help ensure the functions performed are relevant to the scope of the management system all relevant to the subject of the scope expansion.

The focus of the review enabled Schellman to maintain confidence that Microsoft's certified ISMS and PIMS continued to fulfill the requirements of ISO 27001 and ISO 27701 as it pertains to the scope expansion audit. The ISO 27001 scope expansion review included an analysis of the following ISMS and PIMS activities, as applicable:

- internal audits and management review;
- complaints handling;
- effectiveness of the management system with regard to achieving the certified client's objectives and the intended results of the ISMS and PIMS;
- progress of planned activities aimed at continual improvement;
- continuing operational control; and
- review of any changes.

During the assessment, all ISMS and PIMS-related documentation was available for the audit team to assess the ISMS and PIMS and in relation to the audit objectives of this assessment. In addition, there were no deviations from the audit plan, significant issues impacting the audit, or any unresolved issues at the time of the issuance of the report.

A closing meeting occurred remotely utilizing the Microsoft Teams web conferencing application at approximately 10:30 AM PST on Thursday, November 21, 2024. The closing meeting included discussions on the conformity of the client's ISMS and PIMS in relation to the ISO 27001 and ISO 27701 standards, respectively, and discussions regarding the overall scope expansion review recommendation and next steps.

OVERVIEW OF OPERATIONS

Company Background and 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 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 the Appendix.

ISMS AND PIMS REVIEW

Context of the Organization (Clause 4 from ISO 27001 and Clause 5 from ISO 27701)

Understanding the Organization and its Context (ISO 27001 Clause 4.1 and ISO 27701 Clause 5.2.1)

Microsoft recognizes its need to protect critical business information in order to better serve their customers. To achieve this, an ISMS has been created in accordance with the ISO 27001 standard in addition to the control requirements included in the ISMS based on the control sets within the ISO 27017, ISO 27018, and the PIMS processor requirements of ISO 27701. The use of information assets must be in line with good professional working practices and procedures as well as statutory, regulatory, and contractual requirements and must ensure the confidentiality, integrity, and availability of Microsoft's and Microsoft's clients' information assets. Information is an extremely important Microsoft asset and enables Microsoft to fulfill its business functions and obligations to its clients. Microsoft's ISMS helps ensure that Microsoft meets applicable statutory, regulatory, and contractual information security requirements and helps to provide the required client assurances regarding Microsoft's approach to information security.

During the implementation of the ISMS program, the Integrated Management Forum (IMF) identified and established objectives for achieving the intended outcomes of the ISMS and PIMS by evaluating the overall business risks and the ways to mitigate those risks. The ISMS program implementation involved communicating the importance of information security management throughout the organization and clearly outlining and assigning roles and responsibilities to employees who have an effect on the ISMS.

Understanding the Needs and Expectations of Interested Parties (ISO 27001 Clause 4.2 and ISO 27701 Clause 5.2.2)

Microsoft Azure, Dynamics, and other Online Services considers input from the relevant interested parties to determine the obligations and expectations that Microsoft Azure, Dynamics, and other Online Services needs to meet. Microsoft Azure, Dynamics, and other Online Services management engages with the relevant interested parties, on a periodic basis, to discuss the requirements and align Microsoft Azure, Dynamics, and other online Services' plans.

Determining the Scope of the ISMS (ISO 27001 Clause 4.3 and ISO 27701 Clause 5.2.3)

The scope of the ISMS and PIMS is defined and documented and most recently updated as of October 18, 2024, with approval date of October 29, 2024. The scope of the ISMS and PIMS 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 ISMS and PIMS comprises the development, operations and infrastructure teams for Azure and Azure based services deployed in Public, and Government Cloud, collectively referred as Microsoft Azure in accordance with the statement of applicability, version 2024.01, dated January 20, 2024. With respect to the processing of personal information within the scope of the PIMS, Microsoft has determined that it operates as a processor in relation to the services provided to customers.

As part of scope expansion, 36 new service offerings and one set of infrastructure services were added to the scope of the ISMS. The full listing services and offerings are summarized in the Appendix.

Microsoft Azure, Dynamics, and other Online Services applies to information resources, processes, and personnel within the Microsoft Azure, Dynamics, and other Online Services Group. Information resources include any

Microsoft Azure, Dynamics, 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 implementation guidance and control sets of ISO 27017 and ISO 27018 and the management system and control requirements of ISO 27701 as a PII processor.

The only office facility included within the scope of the ISMS and PIMS is the office facility in Redmond, Washington. For a listing of in-scope data centers, see the Appendix.

Information Security Management System (ISO 27001 Clause 4.4 and ISO 27701 Clause 5.2.4)

Microsoft has established an integrated management system (IMS) scope statement which serves as a framework to lead the implementation, maintenance, and continual improvement of the ISMS and PIMS in accordance with the requirements of the standards. Such activities are demonstrated through its establishment of the IMF, which encompasses a select group of Microsoft's department heads to integrate information security considerations into its day-to-day activities, fostering an environment of continual improvement.

Leadership, Objectives, and Support (Clauses 5, 6.2, 6.3, and 7)

The requirements of Clauses 5, 6.2, 6.3, and 7 (Leadership, Objectives, Changes, and Support) are well-defined in the ISMS manual. The following aspects of the ISMS were tested during 2024 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)
- Information Security Objectives and Planning to Achieve Them (Clause 6.2)
- Planning of Changes (Clause 6.3)
- Resources (Clause 7.1)
- Competence (Clause 7.2)
- Awareness (Clause 7.3)
- Communication (Clause 7.4)
- Documented Information (Clause 7.5)

Microsoft's Leadership, Information Security Objectives, Organizational Structure, and Support clauses for its ISMS were not impacted as part of the scope expansion and were documented within the 2024 surveillance review report. As part of the scope expansion, the ISMS clauses were reviewed, and documents were provided to support that they were not impacted.

Planning and Operation (Clauses 6 and 8 from ISO 27001 and Clause 5 from ISO 27701)

Microsoft's leadership ream created the enterprise risk management (ERM) team to identify and ensure accountability of the company's most significant risks. The ERM is structured using a framework based on the COSO (Committee of Sponsoring Organizations of the Treadway Commission) – enterprise risk management integrated framework. It also aligns with the ISO 31000:2009 risk management standard. Microsoft's risk assessment process allows the organization to assess, identify, and modify their overall security posture and to enable security, operations, organizational management, and other personnel to collaborate and view the entire organization from a vulnerability perspective. The risk assessment process has obtained management's commitment for the allocation of resources and for the implementation of appropriate security solutions to achieve the intended outcomes of the ISMS and PIMS, including preventing and mitigating undesired consequences, and continually improving.

Microsoft's process of identifying and assessing risks is a continuous and integrated process, which is integrated into the ongoing management cycles of each service team. The ERM, working in conjunction with the Azure risk management team, analyzes risk registers throughout the year, which are completed at least semi-annually (April and October updates), or when significant events occur. Risk treatment activities are monitored on an ongoing basis to ensure risks are addressed and treatment plans are successfully executed.

Microsoft has established a risk and exception management standard operating procedure (SOP) which documents the Azure risk management program. Risk assessments are performed by Global Azure teams to review the effectiveness of existing controls and safeguards as they pertain to information security and privacy, as well as to identify new risks. These assessments ensure policies and supporting procedures properly address the environment considering changing regulatory, contractual, business, technical, and operational requirements.

As part of the scope expansion to include Microsoft Azure's new offerings and services, an information security risk assessment was performed for each new service to account for the related risks. The risk assessment results were collected and maintained within the risk manager system and the compliance tool and were reviewed and approved to ensure that risk treatment was carried out as necessary per the risk treatment plans. The most recent information security risk assessment and risk treatment processes related to services relevant for the scope expansion took place between September 2023 and September 2024.

A statement of applicability, version 2024.01, has been documented and lists the applicable controls from Annex A of ISO 27001:2022, 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 justification for such exclusion. Per the statement of applicability, Microsoft does not outsource any development activities, and as a result, Annex A control 8.30 (outsourced development) 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 conformance with the requirements of the standard.

Performance Evaluation (Clause 9)

Monitoring, Measurement, Analysis, and Evaluation (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.

Senior leadership reviews and amends the security KPIs and major milestones as part of the semester planning (green light) process on a semi-annual basis. KPIs are reviewed by management and action items are created and tracked via appropriate security metrics through the S360 portal. Additionally, KPI monitoring and measurement discussions are held during the quarterly compliance and privacy review meetings.

Internal Audit (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. The compliance team coordinates and facilitates the independent attestations/reviews. Internal audits are performed by third-party auditors from Ernst and Young.

The most recent internal audit efforts occurred as of March 2024, with the internal audit report issued in April 2024. The results of ISMS internal audit activities are communicated to the relevant interested parties and are reviewed by members of ISMS management.

Compliance assessments were conducted surrounding the additional services and offerings as it pertained to the ISMS framework and applicable controls (including the ISO 27701 processor control activities) by the Microsoft

compliance onboarding team. Schellman reviewed the compliance assessment reports for a representative sample of services and offerings as part of scope expansion review, which was found to be in conformance with the requirements of the standard.

Management Review (Clause 9.3)

Monthly cloud and artificial intelligence (CAI) leadership reviews are conducted to discuss progress, monitor changes, and provide input to continuous improvement of the security and privacy KPIs. Leadership reviews ensure the continuing suitability, adequacy, and effectiveness of the 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.

The most recent monthly CAI leadership review meeting was held on October 7, 2024. Minutes were taken during the meeting and maintained as records. The minutes included the agenda items, the associated action items, and future management review meeting topics to be discussed, and incorporated the considerations of the additional services and offerings.

The performance evaluation process was noted to have been effectively implemented related to the additional services and offerings in conformance with the requirements of the standard.

Improvement (Clause 10)

The requirements of Clause 10 (continual improvement and corrective action) are 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:

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

PIMS-Specific Process Assessment

The controls of Clauses 8.2-8.5 (B.8.2-B.8.5) are well-defined in the data processing addendum (DPA), DPIA, and the Service Trust Portal. The following aspects of the PIMS were tested during the 2024 scope expansion review and were noted to be unchanged during the scope expansion review:

- Customer Agreement (Clause 8.2.1)
- Organization's Purposes (Clause 8.2.2)
- Marketing and Advertising Use (Clause 8.2.3)
- Infringing Instructions (Clause 8.2.4)
- Customer Obligations (Clause 8.2.5)
- Records Related to Processing PII (Clause 8.2.6)
- Obligations to PII Principals (Clause 8.3.1)
- Temporary Files (Clause 8.4.1)
- Return, Transfer, or Disposal of PII (Clause 8.4.2)
- PII Transmission Controls (Clause 8.4.3)
- Basis for PII Transfer Between Jurisdictions (Clause 8.5.1)
- Countries and International Organizations to Which PII Can be Transferred (Clause 8.5.2)
- Records of PII Disclosures to Third Parties (Clause 8.5.3)
- Notification of PII Disclosure Requests (Clause 8.5.4)

- Legally Binding PII Disclosures (Clause 8.5.5)
- Disclosure of Subcontractors Used to Process PII (Clause 8.5.6)
- Engagement of a Subcontractor to Process PII (Clause 8.5.7)
- Change of Subcontractor to Process PII (Clause 8.5.8)

Microsoft's PIMS clauses were not impacted as part of the scope expansion and were documented within the 2024 ISO 27001 surveillance review report. As part of the scope expansion, the PIMS clauses were reviewed, and documents were provided to support that they were not impacted.

SECTION 3

SCOPE EXPANSION REVIEW TESTING RESULTS

TEST RESULT CLASSIFICATIONS

Explanation of ISO Requirement Classifications

This report provides management with an 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 and the control activities identified within Annex A, ISO 27017, ISO 27018, and ISO 27701, that are applicable to the ISMS. In addition, this report provides management with an identification of the documentation efforts, in addition to the review and testing of the maintenance, monitoring, and operating effectiveness of the PIMS in relation to the ISO 27701 standard requirements, specifically Clauses 5 through 8 and the control activities identified within Annex B that are applicable to the PIMS. 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 (N/A)** – The Clause was not applicable to the review.

SCOPE EXPANSION REVIEW TESTING RESULTS

Clause	Subject Audited	Clause Classification				Remarks
		C	MN	MJ	NA	
ISO 27001 ISMS Clause Requirements						
4.1	Understanding the organization and its context	ü				
4.2	Understanding the needs and expectations of interested parties	ü				
4.3	Determining the scope of the information security management system	ü				
4.4	Information security management system	ü				
5.1	Leadership and commitment				ü	Note 1
5.2	Policy				ü	Note 1
5.3	Organizational roles, responsibilities, and authorities				ü	Note 1
6.1	Actions to address risks and opportunities	ü				
6.2	Information security objectives and planning to achieve them				ü	Note 1
6.3	Planning of changes				ü	Note 1
7.1	Resources				ü	Note 1
7.2	Competence				ü	Note 1
7.3	Awareness				ü	Note 1
7.4	Communications				ü	Note 1
7.5	Documented information				ü	Note 1
8.1	Operational planning and control	ü				
8.2	Information security risk assessment	ü				
8.3	Information security risk treatment	ü				
9.1	Monitoring, measurement, analysis, and evaluation	ü				
9.2	Internal audit	ü				
9.3	Management review	ü				
10.1	Continual improvement				ü	Note 1
10.2	Nonconformity and corrective action				ü	Note 1

Clause	Subject Audited	Clause Classification				Remarks
		C	MN	MJ	NA	
ISO 27001 Annex A Control Objectives						
Organizational Controls						
5.1[1,2,3]	Policies for information security				ü	Note 2
5.2[1,2,3]	Information security roles and responsibilities				ü	Note 2
5.3	Segregation of duties				ü	Note 2
5.4	Management responsibilities				ü	Note 2
5.5[2]	Contact with authorities				ü	Note 2
5.6	Contact with special interest groups				ü	Note 2
5.7	Threat intelligence	ü				
5.8[2]	Information security in project management	ü				
5.9[2]	Inventory of information and other associated assets				ü	Note 2
5.10	Acceptable use of information and other associated assets				ü	Note 2
5.11	Return of assets				ü	Note 2
5.12[3]	Classification of information				ü	Note 2
5.13[2,3]	Labelling of information				ü	Note 2
5.14[1,3]	Information transfer	ü				
5.15[2]	Access control	ü				
5.16[1,2,3]	Identity management	ü				
5.17[2]	Authentication information	ü				
5.18[1,2,3]	Access rights	ü				
5.19[2]	Information security in supplier relationships				ü	Note 2
5.20[2,3]	Addressing information security within supplier agreements				ü	Note 2
5.21[2]	Managing information security in the ICT supply chain				ü	Note 2
5.22	Monitoring, review, and change management of supplier services				ü	Note 2
5.23	Information security for use of cloud services	ü				
5.24[1,2,3]	Information security incident management planning and preparation	ü				
5.25	Assessment and decision on information security events	ü				

Clause	Subject Audited	Clause Classification				Remarks
		C	MN	MJ	NA	
5.26[3]	Response to information security incidents	ü				
5.27	Learning from information security incidents	ü				
5.28[2]	Collection of evidence	ü				
5.29	Information security during disruption	ü				
5.30	ICT readiness for business continuity	ü				
5.31[2,3]	Legal, statutory, regulatory, and contractual requirements				ü	Note 2
5.32[2]	Intellectual property rights				ü	Note 2
5.33[2,3]	Protection of records				ü	Note 2
5.34[2]	Privacy and protection of PII				ü	Note 2
5.35[1,2,3]	Independent review of information security				ü	Note 2
5.36[3]	Compliance with policies, rules, and standards for information security				ü	Note 2
5.37	Documented operating procedures				ü	Note 2
People Controls						
6.1	Screening				ü	Note 2
6.2	Terms and conditions of employment				ü	Note 2
6.3[1,2,3]	Information security awareness, education, and training				ü	Note 2
6.4	Disciplinary process				ü	Note 2
6.5	Responsibilities after termination or change of employment				ü	Note 2
6.6[3]	Confidentiality or non-disclosure agreements				ü	Note 2
6.7	Remote working	ü				
6.8[2]	Information security event reporting	ü				
Physical Controls						
7.1	Physical security perimeters				ü	Note 2
7.2	Physical entry				ü	Note 2
7.3	Securing offices, rooms, and facilities				ü	Note 2
7.4	Physical security monitoring				ü	Note 2
7.5	Protecting against physical and environmental threats				ü	Note 2
7.6	Working in secure areas				ü	Note 2
7.7[3]	Clear desk and clear screen				ü	Note 2

Clause	Subject Audited	Clause Classification				Remarks
		C	MN	MJ	NA	
7.8	Equipment siting and protection				ü	Note 2
7.9	Security of assets off premises				ü	Note 2
7.10[3]	Storage media				ü	Note 2
7.11	Supporting utilities				ü	Note 2
7.12	Cabling security				ü	Note 2
7.13	Equipment maintenance				ü	Note 2
7.14[1,2,3]	Secure disposal or re-use of equipment				ü	Note 2
Technological Controls						
8.1[3]	User endpoint devices	ü				
8.2[2]	Privileged access rights	ü				
8.3[2]	Information access restriction	ü				
8.4	Access to source code	ü				
8.5[1,3]	Secure authentication	ü				
8.6[2]	Capacity management	ü				
8.7	Protection against malware	ü				
8.8[2,3]	Management of technical vulnerabilities	ü				
8.9	Configuration management	ü				
8.10	Information deletion				ü	Note 2
8.11	Data masking	ü				
8.12	Data leakage prevention	ü				
8.13[1,2,3]	Information backup	ü				
8.14	Redundancy of information processing facilities	ü				
8.15[1,2,3]	Logging	ü				
8.16	Monitoring activities	ü				
8.17[2]	Clock synchronization	ü				
8.18[2]	Use of privileged utility programs	ü				
8.19	Installation of software on operational systems	ü				
8.20	Networks security	ü				
8.21	Security of network services	ü				
8.22[2]	Segregation of networks	ü				
8.23	Web filtering	ü				
8.24[1,2,3]	Use of cryptography	ü				

Clause	Subject Audited	Clause Classification				Remarks
		C	MN	MJ	NA	
8.25[2,3]	Secure development life cycle	ü				
8.26[3]	Application security requirements	ü				
8.27[3]	Secure system architecture and engineering principles	ü				
8.28	Secure coding	ü				
8.29[2]	Security testing in development and acceptance	ü				
8.30[3]	Outsourced development	ü				
8.31[1]	Separation of development, test, and production environments	ü				
8.32[2]	Change management	ü				
8.33[3]	Test information	ü				
8.34	Protection of information systems during audit testing				ü	Note 2
ISO 27017 Extended Control Set for Cloud Services Security						
CLD.6.3	Relationship Between Cloud Service Customer and Cloud Service Provider				ü	Note 2
CLD.8.1	Responsibility for Assets				ü	Note 2
CLD.9.5	Access Control of Cloud Service Customer Data in Shared Virtual Environment	ü				
CLD.12.1	Operational Procedures and Responsibilities	ü				
CLD.12.4	Logging and Monitoring	ü				
CLD.13.1	Network Security Management	ü				
ISO 27018 Extended Control Set for PII Protection						
A.2	Consent and Choice				ü	Note 2
A.3	Purpose legitimacy and specification				ü	Note 2
A.5	Data minimization				ü	Note 2
A.6	Use, retention, and disclosure				ü	Note 2
A.8	Openness, transparency, and notice				ü	Note 2
A.10	Accountability				ü	Note 2
A.11	Information security				ü	Note 2
A.12	Privacy compliance				ü	Note 2
ISO 27701 PIMS Clause Requirements						
5.2	Context of the organization	ü				
5.4	Planning	ü				

Clause	Subject Audited	Clause Classification				Remarks
		C	MN	MJ	NA	
ISO 27701 Annex B Extended Control Set for PII Processors						
B.8.2	Conditions for Collection and Processing				ü	Note 1
B.8.3	Obligations to PII Principals				ü	Note 1
B.8.4	Privacy by Design and Privacy Default				ü	Note 1
B.8.5	PII Sharing, Transfer and Disclosure				ü	Note 1

Legend

[1] – controls that included additional guidance, and subsequent testing, applicable to supplemental control guidance from ISO 27017
[2] – controls that included additional guidance, and subsequent testing, applicable to supplemental control guidance from ISO 27018
[3] – controls that included additional guidance, and subsequent testing, applicable to supplemental control guidance from ISO 27701

Note 1 – During the scope expansion fieldwork, documents were reviewed to support that the noted clause was not impacted by the scope expansion review. Therefore, with no change for the requirement or control relevant to the scope expansion, the testing Conclusion was deemed Not Applicable.

Note 2 – Annex A domain / control was not sampled as part of the 2024 scope expansion review.

SECTION 4

CERTIFICATION CYCLE PROGRAM

CERTIFICATION CYCLE PROGRAM

Year	Type of Review	Processes to be Assessed	Locations to be Assessed	Dates
2023	Recertification	· ISMS framework (clauses 4-10) · Annex A (A5-A18 / 5-8): o Annex A additional ISO 27017, ISO 27018, and ISO 27701 implementation guidance o Site-specific Annex A controls for locations to be assessed o Transition to ISO 27001:2022 · PIMS framework (Clause 5 and 8) · ISO 27017 extended control set for cloud services security · ISO 27018 extended control set for PII protection (A02-A12) · ISO 27701 Annex B Control Testing for PII Processors (B.8.2-B.8.5)	Remote / Redmond, WA, and Sampled Data Centers	March – April 2023
2023	Scope Expansion	· ISMS framework (clauses 4-10) · Annex A (5-8) sampled control objectives, including Annex A additional ISO 27017, 27018, and ISO 27701 implementation guidance · PIMS framework (Clause 5 and 8) · Sampled ISO 27017 Extended Control Set for Cloud Services Security (CLD.9.5.1; CLD.9.5.2; CLD.12.1; CLD.12.4; CLD.13.1.4) · ISO 27701 Annex B Control Testing for PII Processors (B.8.2-B.8.5)	Remote / Redmond, WA	October – November 2023

Year	Type of Review	Processes to be Assessed	Locations to be Assessed	Dates
2024	Surveillance	· ISMS framework (clauses 4-10) · Annex A (5-8) sampled controls: o Logging and monitoring; development and change management; incident response and disaster recovery o Annex A additional ISO 27017, ISO 27018, and ISO 27701 implementation guidance o Site-specific Annex A controls for locations to be assessed · PIMS framework (Clause 5 and 8) · Sampled ISO 27017 Extended Control Set for Cloud Services Security (CLD.9.5.1, CLD.9.5.2, CLD.12.1, CLD.12.4) · Sampled ISO 27018 extended control set for PII protection (A02-A07) · ISO 27701 Annex B Control Testing for PII Processors (B.8.2, B.8.4)	Remote / Redmond, WA, and Sampled Data Centers	February - March 2024
2024	Scope Expansion	· ISMS framework (clauses 4-10) · Annex A (5-8) sampled control objectives, including Annex A additional ISO 27017, 27018, and ISO 27701 implementation guidance · PIMS framework (Clause 5 and 8) · Sampled ISO 27017 Extended Control Set for Cloud Services Security (CLD.9.5.1; CLD.9.5.2; CLD.12.1; CLD.12.4; CLD.13.1.4) · ISO 27701 Annex B Control Testing for PII Processors (B.8.2-B.8.5)	Remote / Redmond, WA	October 2024
2025	Surveillance	· ISMS, PIMS, and specific scope testing surrounding operations	· Redmond, WA, and Sampled Data Centers	March 2025
2026	Recertification	· ISMS, PIMS, and full system scope	· Redmond, WA, and Sampled Data Centers	March – April 2026

Legend

☐ Future projects

APPENDIX

MICROSOFT AZURE SCOPE STATEMENT

MICROSOFT AZURE SCOPE STATEMENT

Scope of the ISMS and PIMS

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

Microsoft: Azure, Dynamics, and other Online Services IMS applies to information resources, processes, and personnel within the Microsoft: Azure, Dynamics, and other Online Services Group. Information Resources include any Microsoft: Azure, Dynamics, 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

The IMS scope includes selective Microsoft: Azure, Dynamics, and other Online Services noted below that are deployed in Azure Public and Government Cloud including their development and operations, infrastructure and their associated security, privacy, and compliance:

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
AI + Machine Learning	Azure Bot Service	✓	✓
	Azure Open Datasets	✓	-
	Azure AI Services	✓	✓
	Azure AI Services: Azure AI Anomaly Detector	✓	-
	Azure AI Services: Azure AI Document Intelligence	✓	✓
	Azure AI Services: Azure AI Metrics Advisor	✓	-
	Azure AI Services: Azure AI Vision	✓	✓
	Azure AI Services: Azure AI Content Safety	✓	✓
	Azure AI Services: Azure AI Content Moderator	✓	✓
	Azure AI Services: Azure AI Custom Vision	✓	✓
	Azure AI Services: Azure AI Face	✓	✓
	Azure AI Services: Azure AI Immersive Reader	✓	-
	Azure AI Services: Azure AI Personalizer	✓	✓
	Azure AI Services: Azure AI Language	✓	✓
	Azure AI Services: Azure AI Language Understanding	✓	✓
	Azure AI Services: Azure AI Translator	✓	✓

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
AI + Machine Learning	Azure AI Services: Azure AI QnA Maker	✓	✓
	Azure AI Services: Azure AI Speech	✓	✓
	Azure AI Services: Azure AI Video Indexer	✓	✓
	Azure AI Services: Azure AI Search	✓	✓
	Azure AI Studio	✓	-
	Azure Machine Learning	✓	✓
	AI Builder	✓	✓
	Azure Machine Learning Studio	✓	-
	Microsoft Genomics	✓	-
	Microsoft Autonomous Development Platform	✓	-
	Microsoft Security Copilot	✓	-
	Microsoft Copilot for Sales	✓	-
	Microsoft Copilot for Service	✓	-
	Azure Health Bot	✓	-
	Azure Open AI Service	✓	-
	Azure Health AI Deidentification Service	✓	-
	Azure Singularity	✓	-
	Azure OpenAI Services	✓	-
Analytics	Azure Analysis Services	✓	✓
	Azure Chaos Studio	✓	-
	Azure Data Explorer	✓	✓
	Azure Data Factory	✓	✓
	Azure HDInsight	✓	✓
	Azure Operator Service Manager	✓	-
	Azure Stream Analytics	✓	✓
	Data Catalog	✓	-
	Data Lake Analytics	✓	-
	Azure Data Share	✓	✓
	Azure Operator Insights	✓	-
	Microsoft Fabric	✓	-
	Healthcare Data Solutions in Microsoft Fabric	✓	-

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
Analytics	Power BI Embedded	✓	✓
	Azure Usage Billing	✓	-
Compute	Cloud Services (Extended Support)	✓	✓
	Service Fabric	✓	✓
	Virtual Machine Scale Sets	✓	✓
	Virtual Machines	✓	✓
	Virtual Machines Licenses	✓	-
	Virtual Machines Bav2 Series	✓	✓
	Virtual Machines Bv2 Series	✓	✓
	SQL Server on Azure Virtual Machines	✓	✓
	Virtual Machine Extensions	✓	✓
	Batch	✓	✓
	Azure Functions	✓	✓
	App Service	✓	✓
	App Service – Web Apps (including Containers)	✓	✓
	App Service – API Apps	✓	✓
	App Service – Mobile Apps	✓	✓
	App Service – Static Web Apps	✓	✓
	Service Connector	✓	-
	Azure AutoManage Machine Configuration	✓	✓
	Azure VMware Solution	✓	✓
	Planned Maintenance	✓	✓
	Azure Arc-enabled Servers	✓	✓
	Azure VM Image Builder	✓	✓
	Azure Virtual Desktop	✓	✓
	Azure Spring Apps	✓	-
	Azure Center for SAP Solutions	✓	-
	Azure Large Instances	✓	-
	Azure Large Instance for Epic v1.1	✓	-
	NVIDIA Omniverse on Azure	✓	-
	Azure Modeling and Simulation Workbench	✓	-

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
Compute	Azure Service Manager (RDFE)	✓	✓
Containers	Azure Kubernetes Service (AKS)	✓	✓
	Azure Arc-enabled Kubernetes	✓	✓
	Azure Kubernetes Configuration Management	✓	✓
	Azure Red Hat OpenShift (ARO)	✓	✓
	Container Instances	✓	✓
	Azure Container Registry	✓	✓
	Azure Container Storage	✓	✓
	Azure Container Apps	✓	✓
	Microsoft Container Registry	✓	-
	Azure Kubernetes Fleet Manager	✓	✓
Databases	Azure Arc-enabled SQL Server	✓	-
	SQL Managed Instance enabled by Azure Arc	✓	-
	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	✓	✓
	Azure Synapse Analytics	✓	✓
	Azure SQL Edge	✓	-
	Azure Managed Instance for Apache Cassandra	✓	-
	Oracle Database@Azure**	✓	-
	Azure SQL Managed Instance	✓	✓
Developer Tools	Azure DevTest Labs	✓	✓
	Azure Lab Services	✓	✓
	Azure for Education	✓	-
	Azure App Configuration	✓	✓
	Azure Load Testing	✓	✓
	Azure Deployment Environments	✓	-

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
Developer Tools	Microsoft Dev Box	✓	-
Hybrid + Multicloud	Azure Arc-enabled System Center Virtual Machine Manager	✓	-
	Azure Arc-enabled VMware vSphere	✓	-
	Azure Arc-enabled VMware Solution	✓	-
	Azure Arc User Experiences	✓	✓
	Azure Stack*	✓	✓
	Nutanix on Azure	✓	-
Identity	Azure Information Protection	✓	✓
	Microsoft Entra ID	✓	✓
	Microsoft Entra ID Governance	✓	-
	Microsoft Global Secure Access	✓	-
	Microsoft Accounts	✓	-
	Azure Active Directory B2C	✓	✓
	Microsoft Entra Domain Services	✓	✓
Integration	Logic Apps	✓	✓
	API Management	✓	✓
	Azure API Center	✓	-
	Service Bus	✓	✓
	Azure Health Data Services	✓	✓
	Azure Data Manager for Energy	✓	-
Internet of Things	Event Hubs	✓	✓
	Event Grid	✓	✓
	Azure Internet of Things (IoT) Central	✓	-
	Azure IoT Hub	✓	✓
	Notification Hubs	✓	✓
	Azure Sphere	✓	-
	Azure Time Series Insights	✓	-
	Azure Defender for IoT	✓	✓
	Azure Digital Twins	✓	-
	Device Update for IoT Hub	✓	-

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
Management and Governance	Application Change Analysis	✓	-
	Azure Resource Manager	✓	✓
	Automation	✓	✓
	Azure Advisor	✓	✓
	Azure Lighthouse	✓	✓
	Azure Managed Applications	✓	✓
	Azure Migrate	✓	✓
	Azure Monitor	✓	✓
	Azure Monitor for SAP solutions	✓	-
	Azure Policy	✓	✓
	Azure Resource Graph	✓	✓
	Cloud Shell	✓	✓
	Microsoft Azure Portal	✓	✓
	Defender External Attack Surface Management (EASM)	✓	-
	Azure Blueprints	✓	-
	Cost Management	✓	✓
	Azure Signup Portal	✓	✓
	Resource Move	✓	✓
	Quota + Usage Blade	✓	✓
	Quota Management	✓	✓
	Microsoft Purview (Governance)	✓	✓
	Azure Update Manager	✓	-
	Azure Help	✓	-
	Azure Business Continuity Center	✓	-
	SaaS API	✓	-
	Publisher Verification Service and Application Consent Service	✓	-
	Azure Managed Grafana	✓	-
Media	Azure Media Services	✓	✓
Mixed Reality	Azure Spatial Anchors	✓	-
	Azure Remote Rendering	✓	-

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
Networking	Application Gateway	✓	✓
	Azure Load Balancer	✓	✓
	Microsoft Azure Peering Service	✓	✓
	Azure ExpressRoute	✓	✓
	Virtual Network	✓	✓
	VPN Gateway	✓	✓
	Azure Bastion	✓	✓
	Azure DDoS Protection	✓	✓
	Azure DNS	✓	✓
	Azure Firewall	✓	✓
	Azure Firewall Manager	✓	✓
	Azure Front Door	✓	✓
	Azure Internet Analyzer	✓	-
	Azure Private Link	✓	✓
	Azure Private MEC	✓	-
	Azure Web Application Firewall	✓	✓
	Content Delivery Network	✓	✓
	Network Watcher	✓	✓
	Traffic Manager	✓	✓
	Virtual WAN	✓	✓
	IP Services	✓	✓
	Virtual Network NAT	✓	✓
	Azure Communications Gateway	✓	-
	Azure Operator Nexus	✓	-
	AFOI-Network Cloud	✓	-
	Azure Orbital Ground Station	✓	-
	Azure Network Function Manager	✓	✓
	Azure Route Server	✓	✓
	Azure Virtual Network Manager	✓	-
	Azure ExpressRoute Traffic Collector	✓	-
Security	Key Vault	✓	✓

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
Security	Azure Payment HSM	✓	-
	Multi-Factor Authentication	✓	✓
	Azure Dedicated HSM	✓	✓
	Customer Lockbox for Microsoft Azure	✓	✓
	Microsoft Sentinel	✓	✓
	Microsoft Defender for Cloud	✓	✓
	Microsoft Azure Attestation	✓	-
	Azure Confidential Ledger	✓	-
	Trusted Hardware Identity Management	✓	-
Storage	Storage (Blobs (including Azure Data Lake Storage Gen 2), Disks, Files, Queues, Tables, Azure Disk Storage) including Cool and Premium	✓	✓
	Azure Storage Mover	✓	-
	Azure Archive Storage	✓	✓
	Azure Data Box	✓	✓
	Azure HPC Cache	✓	✓
	Azure Site Recovery	✓	✓
	StorSimple	✓	✓
	Azure Backup	✓	✓
	Azure File Sync	✓	✓
	Azure NetApp Files	✓	✓
	Azure Files	✓	✓
	Azure Elastic SAN	✓	-
	Azure Managed Lustre	✓	✓
Web	Azure Cognitive Search	✓	✓
	Azure Fluid Relay	✓	✓
	Azure Maps	✓	✓
	Azure SignalR Service	✓	✓
	Azure Web PubSub	✓	✓

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
Microsoft Online Services			
Commercial Marketplace Public Storefront		✓	-
Intelligent Recommendations		✓	-
Microsoft Copilot Studio		✓	✓
Microsoft Intune		✓	✓
Microsoft Defender for Cloud Apps		✓	✓
Microsoft Defender Threat Intelligence		✓	-
Microsoft Graph		✓	✓
Microsoft Managed Desktop		✓	-
Microsoft Stream		✓	✓
Power Apps		✓	✓
Power Automate		✓	✓
Power BI		✓	✓
Power Virtual Agents		✓	✓
Microsoft Threat Experts		✓	-
Nomination Portal		✓	✓
Microsoft 365 Defender		✓	✓
Microsoft Defender for Endpoint		✓	✓
Microsoft Defender for Identity		✓	✓
Microsoft Defender Vulnerability Management		✓	✓
Microsoft Defender Experts for XDR		✓	-
Microsoft Defender Experts for Hunting		✓	-
Microsoft Bing for Commerce		✓	-
Universal Print		✓	-
Update Compliance		✓	-
Azure Managed Experience		✓	-
Windows Autopatch		✓	-
Viva Sales		✓	-
Seeing AI		✓	-
Microsoft Sustainability Manager		✓	-
Sustainability Data Services		✓	-

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
Online Experimentation		✓	-
Community Training		✓	-
Nuance Conversational IVR		✓	✓
Microsoft Bot Framework		✓	-
Microsoft Secure Score		✓	✓
Microsoft Dynamics 365			
Dynamics 365 Contact Center		✓	-
Dynamics 365 Customer Service		✓	✓
Dynamics 365 Customer Insights Engagement Insights		✓	-
Dynamics 365 Customer Voice		✓	✓
Dynamics 365 Field Service		✓	✓
Dynamics 365 Sales		✓	✓
Dynamics 365 Sales Insights		✓	-
Dynamics 365 Customer Insights		✓	✓
Dynamics 365 Business Central		✓	-
Dynamics 365 Human Resources (Operations)		✓	-
Dynamics 365 Finance		✓	✓
Dynamics 365 Fraud Protection		✓	-
Dynamics 365 - Resource Scheduling Optimization		✓	✓
Dynamics 365 Marketing		✓	-
Power Pages		✓	✓
Dynamics 365 Project Service Automation		✓	✓
Dynamics 365 Project Operations		✓	-
Dynamics 365 Supply Chain Management		✓	-
Dynamics 365 Commerce		✓	-
Dynamics 365 Human Resources (Standalone)		✓	-
Dynamics 365 Intelligent Order Management		✓	-
Chat for Dynamics 365		✓	✓
Dynamics 365 – Data Export Service		✓	-
Dynamics 365 Athena – CDS to Azure Data Lake		✓	✓
Dynamics 365 Guides		✓	-

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
Dynamics 365 Business Q&A		✓	-
Dynamics 365 Remote Assist		✓	✓
Business Copilot AI Offerings		✓	-
Dataverse		✓	✓
Microsoft Cloud for Financial Services			
Unified Customer Profile		✓	-
Collaboration Manager		✓	-
Customer Onboarding		✓	-
Infrastructure Services			
Supporting Infrastructure and Platform Services		✓	✓

Legend

* Includes the Azure Stack Bridge service which provides hybrid capabilities between on-premises Azure Stack deployments and the online Azure cloud; however, customers are responsible for managing the security of on-premises components.

** Azure manages physical security and the Azure platform (Portal, Resource Provider control plane, Identity and Network connectivity) of the Oracle Database@Azure. Oracle Cloud Infrastructure manages the other portions, which include the OCI hardware and control plane.

Physical Environment

Microsoft: Azure, Dynamics, 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 in-scope of the IMS

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 datacenters within scope of the IMS are as follows:

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

Microsoft Azure Domestic Datacenters	
West US	Santa Clara, CA San Jose, CA
West US 2	Columbia, WA Quincy, WA Wenatchee,)
West US 3	Phoenix, AZ
West Central US	Cheyenne, WY
Central US	Des Moines, IA
North Central US	Chicago, IL
South Central US	San Antonio, TX
East US	Bristow, VA Sterling, VA Ashburn, VA Manassas, VA Dulles, VA
East US 2	Boydton, VA Lawrenceville, GA Mecklenburg, NC
US GOV Iowa	Des Moines, IA
US GOV Arizona	Phoenix, AZ
US GOV Texas	San Antonio, TX
US GOV Virginia	Boydton, VA
US GOV Wyoming	Cheyenne, WY

Microsoft Azure International Datacenters	
Canada East	Quebec, Canada
Canada Central	Toronto, Canada
Brazil South	Campinas, Brazil
Brazil Southeast	Rio de Janeiro, Brazil
West Europe	Amsterdam, Netherlands
North Europe	Dublin, Ireland
UK South	London, United Kingdom
UK West	Cardiff, United Kingdom
France Central	Paris, France
France South	Marseille, France
Germany North	Berlin, Germany
Germany West Central	Frankfurt, Germany
Sweden Central	Gavleborg, Sweden

Microsoft Azure International Datacenters	
Sweden South	Malmo, Sweden
Switzerland West	Geneva, Switzerland
Switzerland North	Zurich, Switzerland
Norway East	Oslo, Norway
Norway West	Stavanger, Norway
Poland Central	Warsaw, Poland
Italy North	Milan, Italy
Mexico Central	Queretaro, Mexico
East Asia	Hong Kong
Southeast Asia	Singapore
West India	Mumbai, India
Central India	Pune, India
South India	Chennai, India
Jio India Central	Nagpur, India
Jio India West	Jamnagar, India
Japan West	Osaka, Japan
Japan East	Tokyo, Japan
Korea South	Busan, South Korea
Korea Central	Seoul, South Korea
UAE Central	Abu Dhabi
UAE North	Dubai
Australia East	Sydney, Australia
Australia Southeast	Melbourne, Australia
Australia Central	Canberra, Australia
Australia Central 2	Canberra, Australia
South Africa North	Johannesburg, South Africa
South Africa West	Cape Town, South Africa
Qatar Central	Doha, Qatar
Israel Central	Tel Aviv-Yafo, Israel
Spain Central	Madrid, Spain
New Zealand North	Auckland, New Zealand
Taiwan North	Taipei, Taiwan
Taiwan Northwest	Taipei, Taiwan

Microsoft Online Services Datacenters	
Kuala Lumpur, Malaysia	Vienna, Austria
Johor Bahru, Malaysia	Vantaa, Finland
Busan, South Korea	Cheyenne, WY
Fortaleza, Brazil	Tokyo, Japan
Rio de Janeiro, Brazil	Beijing, China
Santiago, Chile	

Edge Sites	
Athens, Greece	Manila, Philippines
Atlanta, GA	Memphis, TN
Auckland, New Zealand	Miami, FL
Bangkok, Thailand	Milan, Italy
Barcelona, Spain	Minneapolis, MN
Barueri, Brazil	Montreal, Canada
Berlin, Germany	Mumbai, India
Bogota, Colombia	Munich, Germany
Brisbane, Australia	Nairobi, Kenya
Brussels, Belgium	Nashville, TN
Bucharest, Romania	Manchester, United Kingdom
Budapest, Hungary	New Delhi, India
Buenos Aires, Argentina	New York City, NY
Busan, South Korea	Newark, NJ
Cairo, Egypt	Osaka, Japan
Cape Town, South Africa	Oslo, Norway
Chicago, IL	Palo Alto, CA
Cincinnati, OH	Paris, France
Copenhagen, Denmark	Philadelphia, PA
Dallas, TX	Phoenix, AZ
Detroit, MI	Portland, OR
Doha, Qatar	Prague, Czech Republic
Dubai, United Arab Emirates	Pune, India
Dusseldorf, Germany	Queretaro, Mexico
Frankfurt, Germany	Rabat, Morocco
Geneva, Switzerland	Rio De Janeiro, Brazil
Helsinki, Finland	Rome, Italy
Ho Chi Minh City, Vietnam	Salt Lake City, UT

Edge Sites	
Hong Kong	Sao Paulo, Brazil
Honolulu, HI	San Jose, CA
Houston, TX	Seattle, WA
Hyderabad, India	Seoul, South Korea
Istanbul, Turkey	Singapore
Jacksonville, FL	Sofia, Bulgaria
Jakarta, Indonesia	Stockholm, Sweden
Johannesburg, South Africa	Taipei, Taiwan
Kuala Lumpur, Malaysia	Tel Aviv, Israel
Lagos, Nigeria	Teterboro, NJ
Las Vegas, NV	Tokyo, Japan
Lisbon, Portugal	Toronto, Canada
London, United Kingdom	Vancouver, Canada
Los Angeles, CA	Warsaw, Poland
Luanda, Angola	Zagreb, Croatia
Madrid, Spain	Zurich, Switzerland

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.