Microsoft Azure, Dynamics 365 and Online Services

ISO 27001:2013, ISO 27018:2019, ISO 27017:2015, and ISO 27701:2019
Certification - Surveillance Review Summary Report

June 21, 2022

Attestation and Compliance Services

Quality, above all.

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 Surveillance 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 surveillance 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.

Schellman also performed the following reviews for Microsoft's Azure, Dynamics 365, and other Online Services that are deployed in Azure Public and Government Cloud:

- ISO 9001:2015 surveillance review
- ISO/IEC 20000-1:2018 surveillance review
- ISO 22301:2019 recertification review
- Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) surveillance review

Table of Contents

SECTION I

AUDIT TEAM RECOMMENDATION

Audit Team Recommendation

Summary of Findings and Recommendation

Overall, the Information Security Management System (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 and based on the control sets within ISO/IEC 27017:2015 (ISO 27017) and ISO/IEC 27018:2019 (ISO 27018), and the operation and maintenance of the PIMS processor requirements of ISO 27701:2019 (ISO 27701). There were no nonconformities or opportunities for improvement (OFIs) noted as a result of the 2022 surveillance review.

The ISMS and the Privacy Information Management System (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.

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 2022 surveillance 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 surveillance review were met.

SECTION 2

PROJECT OVERVIEW

Executive Summary

Introduction

Microsoft Corporation ("Microsoft" or the "client") underwent a surveillance review in March and April 2022 of their ISO/IEC 27001:2013 ("ISO 27001" or the "standard") certification which was originally issued in November 2011. The purpose of the surveillance review was to verify that the approved ISMS and PIMS continued to be implemented, to consider the implications of changes to that system initiated as a result of changes in the client organization's operations, and to confirm continued compliance with the certification requirements, in addition to the control implementation guidance of ISO 27017 and ISO 27018, as well as the management system requirements, controls and control implementation guidance of ISO 27701 in the role as a personally identifiable information (PII) processor. This report includes the results of the 2022 surveillance review mentioned above.

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

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

The scope of the review was limited to the ISMS supporting Microsoft Azure, Dynamics 365, and other Online Services that are deployed in Azure Public and Government 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/IEC 27701:2019 for a PIMS as data processor per the statement of applicability version 2022.01. The scope of the ISMS includes the control requirements of ISO/IEC 27017:2015 and ISO/IEC 27018:2019. The scope of the ISMS includes the ISMS development, operations and infrastructure teams for Azure and Azure based services deployed in the Public, and Government Cloud, collectively referred as Microsoft Azure, Dynamics, and other Online Services in accordance with its Statement of Applicability, version 2022.01. 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 includes operations at the locations identified in the Appendix.

Opening Meeting Description

An opening meeting occurred remotely utilizing the Microsoft Teams web conferencing application, at approximately 10:30 AM PST on Monday, March 14, 2022. An agenda was provided as well as a project plan for the surveillance review.

The opening meeting was held to perform the following:

- Reconfirm the audit plan, scope, and deliverables for the surveillance 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 surveillance audit covered the documentation requirements of the ISO 27001, ISO 27017, ISO 27018, and ISO 27701 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 surveillance audit objectives included the following:

- Determine the continued conformance of the ISMS to the ISO 27001 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;
- Determine the continued conformance of the PIMS to the ISO 27701 standard, specifically with regard to achieving the objectives of Microsoft's privacy policy and Microsoft's maintenance, monitoring, and improvement activities of the PIMS;
- Effectiveness of the procedures and processed for evaluation and review of compliance with relevant information security legislation and regulations; and
- Review of action taken on OFIs identified during the previous audit.

The audit focused on the client's:

- Internal audits and management review
- A review of actions taken on OFIs identified during the previous audit
- Treatment of complaints
- 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
- Use or marks and/or any reference to certification

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 closing meeting was held remotely utilizing the Microsoft Teams web conferencing application, at approximately 2:30 PM PST on Tuesday, June 21, 2022. The closing meeting included a discussion with the ISMS team regarding the surveillance review findings and the overall surveillance review recommendation and next steps.

Confidentiality Statement

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

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 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 the Appendix.

ISMS and PIMS Review

General Design and Operating Effectiveness of the Client ISMS and PIMS

The general design and operating effectiveness of the ISMS conforms to 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, ISO 27018, and maintenance and operation of the PIMS based on the requirements and control implementation guidance of ISO 27701.

Clause	Conclusion	Comment
Context of the Organization and Additional 27701 Implementation Guidance	Effective	No Comment
Leadership – Commitment	Effective	No Comment
Leadership – Policy	Effective	No Comment
Leadership – Organizational Roles, Responsibilities, and Authorities	Effective	No Comment
Planning – Risk Assessment and Additional 27701 Implementation Guidance	Effective	No Comment
Planning – Risk Treatment and Additional 27701 Implementation Guidance	Effective	No Comment
Planning – Objectives	Effective	No Comment
Support – Resources	Effective	No Comment
Support – Competence	Effective	No Comment
Support – Awareness	Effective	No Comment
Support – Communication	Effective	No Comment
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

Clause	Conclusion	Comment
Improvement – Nonconformity / Corrective Action	Effective	No Comment
Improvement – Continual Improvement	Effective	No Comment
Annex A Control Testing and Additional ISO 27017, ISO 27018, and ISO 27701 Implementation Guidance	Effective	No Comment
ISO 27701 Annex B Control Testing for PII Processors	Effective	No Comment

ISMS and PIMS Maintenance Activities

Overall, Microsoft continued to demonstrate a sound understanding of its ISMS as it continued to meet 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, ISO 27018, and maintenance and operation of the PIMS based on the requirements and control implementation guidance of ISO 27701. During the surveillance review, an assessment was performed to determine the overall effectiveness of the ISMS during the certification lifecycle and no negative trends were identified. The ISMS 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 has implemented continual improvement activities since the 2021 surveillance and 2021 scope expansion review based on results from its risk assessments and implementation of risk treatment plans that were based on available or planned resources that took into consideration external and internal factors such as new organizational changes and location-specific regulations. Further, there have been no complaints and Microsoft has properly marketed their certificate in accordance to the client obligations and marketing guidelines provided to Microsoft.

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 party, 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 March 25, 2022, version 2022.01. 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 2022.01, dated March 25, 2022. 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.

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 requirements of ISO 27017 and ISO 27018 and the management system and control requirements of ISO 27701 as a data 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, Information Security Objectives, Organizational Structure, and Support (Clauses 5, 6, and 7)

Leadership and Commitment (Clause 5.1)

The leadership team provides following support to the ISMS and PIMS:

- Agree on high-level strategies that support the business model behind high-scale Microsoft Azure services;
- Provide required budget to achieve the objectives of the ISMS and PIMS;
- Review scorecards and metrics of Microsoft Azure including periodic cloud and enterprise fundamental meetings; and
- Serve as the escalation point to discuss and reach resolution on cross-organizational issues related to Microsoft Azure.

Microsoft Azure leadership is committed to lead and strategically align the ISMS and PIMS to meet business goals and objectives and their responsibility and commitment to the ISMS and PIMS is demonstrated by:

- Helping ensure that information security and privacy policies and objectives are established and aligned with Microsoft's strategic direction;
- Helping ensure that integration of ISMS and PIMS requirements into the Microsoft processes;
- Helping ensure that resources are available for the support of the ISMS and PIMS;
- Helping ensure that the ISMS and PIMS achieve their intended outcome(s);
- Periodically reviewing the ISMS and PIMS and promoting continual improvement; and
- Encouraging and supporting other management roles to demonstrate leadership within their areas or responsibility.

Policy (Clause 5.2)

The IMF is responsible for establishing information security policies that are in alignment with organizational purpose and provide a framework for setting information security objectives.

The information security policies include commitments:

- To satisfy applicable requirements for information security and privacy; and
- To continually improve the ISMS and PIMS.

Microsoft's information security policies have been developed in alignment with the standards to meet Microsoft's compliance obligations. The information security policies establish the foundation for IT and security to help ensure appropriate and authorized access, usage, and integrity of information. The ISO 27001 Annex A controls 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 serve as the Microsoft standard as well as additional industry controls to meet additional regulatory requirements. Microsoft's information security policies are documented, communicated to the Microsoft workforce, and available to interested parties, as appropriate.

Information Security Objectives (Clause 6.2)

Microsoft has established security and privacy objectives at appropriate and relevant functions and levels to provide a platform to improve security, privacy, delivery, corrective action response, and other metrics to achieve desired performance levels for Microsoft cloud products and services.

The information security objectives are:

- Specified in a way that allows determination of their fulfilment to be made;
- Measurable, if applicable;
- Periodically verified in accordance with the requirements of monitoring, measurement, analysis, and evaluation and updated as appropriate, consistent with the requirements of continual improvement;
- Communicated in accordance with the requirements of communication; and
- Created and controlled in accordance with the requirements of documented information.

Information security objectives are tracked and monitored closely by responsible departmental teams and reported to the IMF, as necessary. A summary of current information security objectives and their performance is also reported and reviewed as part of the quarterly security leadership meetings, which includes a review of information security objective effectiveness and adequacy.

Organizational Roles, Responsibilities, and Authorities (Clause 5.3)

Microsoft senior management ensures responsibilities and authorities for roles relevant to information security are assigned and communicated. Senior management assigns responsibility and authority for:

- Ensuring the ISMS aligns to the requirements of 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; and
- Reporting on the performance of the ISMS and PIMS to senior management.

Microsoft senior management is committed to information security and asserts that every person employed by or on behalf of Microsoft has important responsibilities to maintain the security of Microsoft information and information assets as documented within company policies.

The objective of the IMF is to ensure the operating effectiveness and continual improvement of the ISMS and PIMS. The ISMS and PIMS provide management oversight and guidance via the IMF review and governance meetings.

Organizational charts are in place that define the organizational structure, reporting lines, and authorities. These charts are communicated to employees and updated as needed.

Resources (7.1)

Microsoft management is committed to continual improvement and effectiveness of the ISMS and PIMS. Periodic reviews are scheduled to allocate appropriate budget to meet operational requirements and implement corresponding action for the risk treatment plans. Through the periodic IMF meetings management provides guidance, resources, budget planning to successfully meet the security objectives.

Competence and Awareness (Clauses 7.2 and 7.3)

Microsoft full time employees (FTEs) and contingent staff are required to undergo the mandatory basic security and privacy awareness training that includes security foundations training and/or role-based training annually to ensure competency for their job function. New hires are required to take mandatory training before accessing the system or performing assigned duties. Suppliers are required to complete supplier code of conduct training upon hire. A cloud and enterprise security education and awareness SOP is in place to provide guidance and direction on the security and awareness training process. For security and compliance training program that are delivered to groups outside the organization, CAI partners with education solutions like the My Learning system.

Competence and awareness are also accounted for as part of the internal audit process, which defines that internal auditors providing internal audit services to Microsoft are subject to review and approval based on competency requirements set forth by Microsoft.

Communication (Clause 7.4)

Microsoft management is committed to proper communication with the internal and external stakeholders regarding the state of the ISMS and PIMS. The internal and external stakeholders have been defined and appropriate decisions are made as to who needs to receive what level of detail and when. A formal communication plan has been established and documented within the Microsoft IMS communication plan. The IMS communication plan is reviewed at least annually or as needed for appropriateness.

Documented Information (Clause 7.5)

Microsoft has defined an SOP to ensure the control over creation, approval, distribution, usage, and updates of documents and records used in the ISMS and PIMS. The SOP is applied to documents and records related to the ISMS and PIMS, regardless of whether the documents and records were created internally or whether they are of external origin. The policy encompasses documents and records stored in any format (e.g., paper, audio, video, etc.).

Documents relevant for the ISMS and PIMS are managed to help ensure that:

- Access is granted on as-needed basis upon proper approval from the document owners and validation on retrieval and use; access is revoked when no longer necessary;
- Changes to the documented information is version controlled; and
- Retention and disposition policies are adhered as defined in the documents and records management procedure.

Documents are reviewed and approved at least annually or upon significant change. Documents are updated by the control owners / service team subject matter experts (SMEs) and approved by the compliance lead prior to publication. The change history of the document tracks any changes to the content, including creation date, version number, author, change description, approver, and approval date.

Risk Identification, Risk Assessment, and Risk Treatment (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 work with management across the enterprise to identify and ensure accountability of the company's most significant risks. 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. ERM working in conjunction with the Azure risk management team analyzes risk registers throughout the year, which is 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 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.

The most recent information security risk assessment and risk treatment processes took place in H2 2021 (07.01.2021 – 12.31.2021). The results of the risk assessment and the status of risk treatment plans were also reviewed as a component of the quarterly security leadership review meetings which most recently occurred on March 23, 2022 (semester planning meeting). As such, the risk assessment and risk treatment processes were noted to be designed appropriately and effectively implemented in conformance with the requirements of the standards.

With respect to privacy-related risks specifically, security, privacy, and engineering teams work in conjunction with the risk manager to identify and prioritize remediation of the risks identified as important as part of an annual privacy review process. Those risks and work items are tracked via internal tools for closure and are monitored by leadership as necessary.

ISMS and PIMS Effectiveness Measurements (Clause 9.1)

Effectiveness measurement of the ISMS and PIMS is to help ensure continued adequacy, effectiveness, and efficiency of the program. This is done so by:

- Evaluating the ISMS and PIMS at least annually with internal auditing activities;
- Performing management reviews at least annually;
- Formulating corrective action plans to improve the program; and
- Ensuring continuous improvement is incorporated to mature the ISMS and PIMS.

In addition, 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.

Measurement initiatives were conducted on a regular basis at varied frequencies, depending on the metric being monitored. Achieved metrics were also formally communicated and reviewed as a component of the January 2022 quarterly security leadership review meeting. The meeting also included a review of nonconformities and corrective actions, audit results, fulfillment of information security objectives, and results of the risk assessments and status of risk treatment plans to evaluate the effectiveness of the overall control environment. The monitoring and measurement process was found to be operating effectively and in conformance with the requirements of the standard.

Internal ISMS and PIMS 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.

Microsoft undergoes several independent internal / external entities managed assessments including but not limited to the following:

- Internal audit;
- ISO/IEC 27001 certification for ISMS;
- ISO 22301 certification for Business Continuity Management System (BCMS);
- ISO 9001 certification for quality management system (QMS);
- ISO/IEC 20000-1 certification for Service Management System (SMS);
- CSA STAR certificate for assessing the maturity of the organization;
- Service Organization Control (SOC) 1 and SOC 2 attestations in accordance with the American Institute of Certified Public Accountants (AICPA) governed trust principles for security, confidentiality, processing integrity, privacy, and availability;
- FedRAMP certifies to the National Institute of Standards and Technology (NIST) 800-53 controls; and
- PCI DSS (Payment Card Industry) assessment for Level 1 Service Provider.

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

The purpose of the internal audits is as follows:

- Plan, establish, implement, and maintain audit programs; this includes frequency, methods, responsibilities, planning requirements and reporting;
- Define the audit criteria and scope for each assessment;
- Select the assessors /auditors and conduct assessments that ensure objectivity and impartiality of the assessment process;
- Ensure that the results are reported to relevant stakeholders and management; and
- Retain documented information as evidence for future reference as appropriate.

As part of this surveillance review, the following internal audit reports were provided:

- Azure FY21 H2 ISO/IEC 27001:2013, ISO/IEC 27701:2019, ISO/IEC 22301:2019, ISO/IEC 27018:2019, and GDPR Internal Audit Report, dated June 6, 2022; and
- Azure ISO/IEC 27017:2015 Internal Audit Report, dated June 3, 2022.

Each audit report included the overall conclusion, objective, scope, criteria as well as detailed audit results to support the audit conclusion.

As identified above, the most recent internal audit efforts occurred as of May 2022, with the internal audit reports provided to the audit team on June 17, 2022, which was post surveillance review fieldwork, but prior to reporting. The internal audit process was found to be operating effectively and in conformance with the requirements of the standard.

Management Reviews (Clause 9.3)

As noted previously, the IMF's role is to provide management oversight and guidance on the business operations and effectiveness of the ISMS and PIMS via periodic meetings.

Quarterly security leadership reviews are conducted to discuss progress, monitor changes, and provide input to continuous improvement of the security and privacy KPIs. The leadership reviews ensure the continuing suitability, adequacy, and effectiveness of the ISMS.

The input to the management reviews includes the following:

- ISMS audits and reviews results;
- Risk assessment results;
- Microsoft Azure security and privacy incident report;
- Feedback from interested parties (internal and external);
- Techniques, products, or procedures used to improve ISMS and PIMS performance and effectiveness;
- Status/trends of nonconformities and corrective actions;
- Vulnerabilities or threats not adequately addressed;
- Results from effectiveness measurements;
- Follow-up actions from previous management reviews;
- Changes to the scope or dependencies of the ISMS and PIMS; and
- Recommendations for continual improvements.

The output from the management review includes the following:

- Security, privacy and compliance projects progress and priorities;
- Decisions on actions to improve the effectiveness of the ISMS and PIMS;
- Update of the risk acceptance criteria and the treatment plan;
- Modification of procedures and controls that affect information security and privacy to respond to internal or external events that may impact on the ISMS and PIMS such as:
  - Business requirements;
  - Security requirements;
  - Privacy requirements;
  - Regulatory or legal requirements;
  - Contractual obligations; and
  - Levels of risk and/or criteria for accepting risks;
- Resource needs; and
- Improvement in measuring controls effectiveness.

The most recent quarterly security leadership review meeting was held on January 20, 2022. Minutes were taken during the meeting and maintained as record. The minutes include the agenda items as well as associated action items. The minutes also included any outputs taken from the meetings. The management review process was noted to be designed appropriately and effectively implemented in conformance with the requirements of the standard. The results of the Azure FY21 H2 ISO/IEC 27001:2013, ISO/IEC 27701:2019, ISO/IEC 22301:2019, ISO/IEC 27018:2019, and GDPR Internal Audit Report and Azure ISO/IEC 27017:2015 Internal Audit Report will be reviewed as a component of the Q2 2022 security leadership review meeting.

Corrective Action and Continual Improvement (Clause 10)

Microsoft management takes corrective action, as needed, to eliminate the cause of nonconformities within the scope of the ISMS and PIMS.

The following procedures are followed when taking corrective action and actions are recorded in the Microsoft Azure exception trackers:

- Identify the specific nonconformities;
- Determine the causes of nonconformities;
- Evaluate the need for actions to ensure that nonconformities do not recur;
- Determine and implement the corrective action(s) needed;
- Record results of action(s) taken to remediate the nonconformity; and
- Review the corrective action(s) taken in a subsequent management review as appropriate.

Depending on the nature and severity of the nonconformity, the records of corrective actions are reviewed by management during Microsoft Azure risk management forum.

The corrective action and continuous improvement process and documentation appear to be effective in both design and application. Continuous improvement was inherent in the supporting processes and activities of Microsoft's ISMS and PIMS. Continuous improvement was supported through the most recent risk assessment, review of information security objectives, results from the most recent internal audit, and outputs from the quarterly security leadership meetings. Additionally, the personnel responsible for the ISMS and PIMS continually assess its effectiveness and how the implementation and execution of the ISMS and PIMS can improve.

PIMS-Specific Process Assessment

Conditions for Collection and Processing (ISO 27701 Clause 8.2)

This clause and associated controls in Annex B were not assessed during the 2022 surveillance review.

Obligation to PII Principals (ISO 27701 Clause 8.3)

Microsoft provides customers with administrative tools to locate personal data to respond to data subject access requests. The Azure Data subject request guide for the GPDR and CCPA, provided on the compliance portal, documents how controllers can meet their obligations to PII principals by identifying, accessing, rectifying, restricting, deleting and exporting personal data. The guide also documents the customer's ability to access, delete and export certain system generated logs associated with the end-user's use of Azure. Additional guidance is provided to customers and PII principals for assistance with data subject access requests in regards with Microsoft's support and professional services.

Microsoft provides customers with the "Trusted Cloud: Microsoft Azure security, privacy, compliance, reliability/resiliency, and intellectual property" whitepaper to document security and privacy processes, as well as implemented technical and organizational measures to protect customer data. Additionally, Microsoft provides customers with documentation to use their data subject request case tool / portal in the Microsoft 365 compliance center.

Microsoft complies with reasonable requests by customers to assist with the customer's response to data subject requests. Microsoft provides a data subject request portal, which enables customers to fulfill GDPR and CCPA requests. In addition, Microsoft provides their customers with built-in controls, configuration management tools, and data subject request tools to assist customers in meeting their obligations to PII principals.

Privacy by Design and Privacy by Default (ISO 27701 Clause 8.4)

This clause and associated controls in Annex B were not assessed during the 2022 surveillance review.

PII Sharing, Transfer, and Disclosure (ISO 27701 Clause 8.5)

Basis for PII Transfer between Jurisdictions and Countries and International Organizations to which PII can be Transferred (Clauses 8.5.1 and 8.5.2)

Microsoft informs customers via its product terms (online service terms) of the basis of data transfers between jurisdictions. Specifically, the commercial licensing terms state for the Azure core services that Microsoft stores customer data at rest within the specified geolocation configured by the customer.

Additionally Microsoft's trust center's "Privacy, data location" webpage states that Microsoft will not transfer to any third-party data that you provide to Microsoft through the use of our business cloud services. Also customers' data may be replicated within a selected geographic area for enhanced data durability, but will not be replicated outside of it. Additionally, Microsoft commits to contractual guarantees under EU standard Contractual Clauses.

Microsoft documents the countries and organizations to which data can be transferred for the Azure product and service offering in the "Data Residency in Azure." The data residency documentation contains a list of data centers, location, and availability. Microsoft's DPIA for Azure IaaS includes a data flow diagram that illustrates the countries and regions to which data may be transferred, and links to the global infrastructure region page. Microsoft also maintains a list of all subprocessors, which indicates the service each subprocessor provides and its corporate location.

Records of PII Disclosure to Third Parties, Notification of PII Disclosure Requests, and Legally Binding PII Disclosures (Clause 8.5.3, 8.5.4, and 8.5.5)

Microsoft's DPA states that the organization will not disclose or provide access to any processed data except for under a customer direction, as described by the DPA, or required by law. Additionally, Microsoft will not disclose or provide access to any processed data to law enforcement unless required by law. If a request by law enforcement or third party is received, if able, Microsoft redirects the third-party or law enforcement agency to the customer, unless legally prohibited from doing so. If compelled to disclose or provide access to any processed data to law enforcement, Microsoft notifies the customer and provides a copy of the demand unless legally prohibited from doing so. Microsoft rejects the request unless required by law to comply. The law enforcement requests report details the number of requests received and provides a FAQ on Microsoft' handing of legal requests.

Additionally, in the whitepaper – "Trusted Cloud: Microsoft Azure Security, Privacy , Compliance" Microsoft details their commitments to protection customer data from legal requests. Microsoft details their processes on notification of requests from law enforcement, stating that the organization redirects the government to seek data from enterprise customers themselves when legally permitted. All law enforcement requests arrive at Microsoft through a secure portal, for which only vetted law enforcement agencies receive access. Once Microsoft reviews the demand and determines that it must provide data, the data specified in the valid legal order is provided to law enforcement through the same, secure portal.

Disclosure of Subcontractors Used to Process PII, Engagement of a Subcontractor to Processor PII, and Change of Subcontractor to Process PII (Clauses 8.5.6, 8.5.7, and 8.5.8)

Microsoft discloses its use of subcontractors to process customer data to a customer via its customer portal. Microsoft's online services subprocessor list includes a complete list of the subcontractors it engages and their corporate locations. Microsoft also allows customers to subscribe and receive notification whenever the listing of subcontractors is updated.

Microsoft's DPA provides the contractual requirements for engaging a subcontractor or subprocessor. When engaging a subprocessor, Microsoft contractually requires that the subprocessor may only access customer data to deliver the services Microsoft has engaged them to provide. Additional requirements state that the subprocessor is prohibited from using customer data for any other purpose.

Microsoft ensures that subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by the DPA. Further, the DPA's European Union general data protection regulation terms (Attachment 2) provides, Microsoft will not engage another processor without prior specific or general written authorization of customer. In the case of general written authorization, Microsoft informs the customer of any intended changes concerning the addition or replacement of other processors, thereby giving Customer the opportunity to object to such changes.

Microsoft has executed contracts with its subprocessors requiring the implementation of controls with respect to processing PII. Microsoft's Master Supplier Services Agreement requires subprocessors to:

- Comply with the most current supplier code of conduct, and the most current anti-corruption policy, and another policies or training identified by Microsoft in a SOW or otherwise during the term;
- Process the Personal Data only on documented instructions from Microsoft;
- Ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and
- Take measures required in accordance with industry best practice, and by data protection law related to data security.

When engaging a new subprocessor, Microsoft provides notice to customers, through the online services subprocessor list, and the notification functionality in My Library. Per Microsoft's DPA, Microsoft will give customer notice (by updating the website and provide customer with a mechanism to obtain notice of that update) of any new subprocessor at least 30 days in advance of providing that subprocessor with access to Customer Data. Per the whitepaper, "How does Microsoft handle your data in the cloud," Microsoft commits to publishing the names of any new subprocessors to list on the service trust portal six months in advance of the subprocessor's authorization to perform services that may involve secure access to customer data or fourteen days in advance of potential access to personal data within Microsoft online services.

Control Activities Supporting the ISMS and PIMS

Process walk throughs were performed for the following Annex A control domains and the applicable controls from ISO 27017 / 27018 / 27701 relevant to the ISMS and PIMS:

- Asset Management (A.8)
- Access Control (A.9)
- Physical and Environmental Security (A.11)
- Operations Security (A.12)
- Communications Security (A.13)
- Information Security Incident Management (A.16)
- ISO 27001 Annex A Additional Control Implementation Guidance relevant to 27017 / 27018 / 27701
- ISO 27017 Extended Control Set for Cloud Services Security (CLD.8.1, CLD.9.5.1, CLD.9.5.2, CLD.12.1, CLD.12.4, CLD.13.1)
- ISO 27018 Extended Control Set for PII Protection (A.2-A.12)
- ISO 27701 Annex B for PII Processors (B.8.3 and B.8.5)

Physical and Environmental Security

As a component of the 2021 ISO 27001 surveillance review, an assessment was performed on a sample selection of in-scope locations. Seven (7) data center facilities were assessed according to the control guidance of Annex 11 – Physical and Environmental Security. Each assessment included an evaluation of related physical security controls as well as environmental security controls for each of the sampled sites. The following sites were included in the 2022 assessment:

- CBR23
- CPQ23
- CWL20
- DM3
- MWH04
- SAT21
- SIN22

No issues were noted as a result of the assessment; however, due to the sensitivity of the evaluation, details were not included in this summary report.

Findings of Nonconformity and Opportunities for Improvement

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

No nonconformities or OFIs were noted during the 2022 surveillance review.

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 (NA)** – Clause or control was not applicable to the review performed.

SECTION 3

SURVEILLANCE REVIEW TESTING RESULTS

SURVEILLANCE 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	✓				
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	✓				
5.2	Policy	✓				
5.3	Organizational roles, responsibilities, and authorities	✓				
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	✓				
7.2	Competence	✓				
7.3	Awareness	✓				
7.4	Communications	✓				
7.5.1	Documented information – general	✓				
7.5.2	Documented information – creating and updating	✓				
7.5.3	Control of documented information	✓				
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	✓				
10.1	Nonconformity and corrective action	✓				
10.2	Continual improvement	✓				

Clause	Subject Audited	Clause Classification				Remarks
		C	MN	MJ	NA	
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	✓				
A.9*^#	Access control	✓				
A.10*^#	Cryptography				✓	Note 1
A.11*^#	Physical and environmental security	✓				
A.12*^#	Operations security	✓				
A.13*^#	Communications security	✓				
A.14^#	Systems acquisition, development, and maintenance				✓	Note 1
A.15^#	Supplier relationships				✓	Note 1
A.16*^#	Information security incident management	✓				
A.17	Information security aspects of business continuity management				✓	Note 1
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	✓				
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	✓				
A.3	Purpose legitimacy and specification	✓				
A.5	Data minimization	✓				
A.6	Use, retention, and disclosure	✓				
A.8	Openness, transparency, and notice	✓				
A.10	Accountability	✓				
A.11	Information security	✓				

Clause	Subject Audited	Clause Classification				Remarks
		C	MN	MJ	NA	
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				✓	Note 1
B.8.3	Obligations to PII Principals	✓				
B.8.4	Privacy by Design and Privacy Default				✓	Note 1
B.8.5	PII Sharing, Transfer and Disclosure	✓				

Legend

Note that Annex A control objectives 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.

Note 1 – Control objective was not selected for testing during the 2022 surveillance review. Refer to Section 4 “Certification Cycle Program” below for details regarding the test plan.

SECTION 4

CERTIFICATION CYCLE PROGRAM

Certification Cycle Program

Year	Type of Review	Processes to be Assessed	Locations to be Assessed	Planned / Applied Audit Time	Dates
2020	Recertification	• ISMS framework (clauses 4-10) • Annex A (A5-A18) ◦ Annex A additional ISO 27017, ISO 27018, and ISO 27701 implementation guidance ◦ Site-specific Annex A controls for locations to be assessed • 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	14 days remote auditing / 2 days planning and reporting	March – April 2020
2020	Scope Expansion	• ISMS framework (clauses 4-10) • Annex A sampled control objectives: ◦ A.9 ◦ A.12 ◦ A.13 ◦ A.14 ◦ A.17 ◦ Annex A additional ISO 27017, 27018, and ISO 27701 implementation guidance • PIMS framework (Clause 5 and 8) • 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	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	• ISMS framework (clauses 4-10) • Annex A sampled control objectives: • A.5 • A.6 • A.10 • A.11 • A.14 • A.15 • A.17 • A.18 • Annex A additional ISO 27017, 27018, and ISO 27701 implementation guidance • 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.6.3 • 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	18 days remote auditing / 5.5 days planning and reporting	April 2021

Year	Type of Review	Processes to be Assessed	Locations to be Assessed	Planned / Applied Audit Time	Dates
2021	Scope Expansion	• ISMS framework (clauses 4-10) • Annex A sampled control objectives: • A.9 • A.12 • A.13 • A.14 • A.17 • 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	15 days remote auditing / 4 days planning and reporting	October – November 2021

Year	Type of Review	Processes to be Assessed	Locations to be Assessed	Planned / Applied Audit Time	Dates
2022	Surveillance	• ISMS framework (clauses 4-10) • Annex A sampled control objectives: • A.8 • A.9 • A.11 • A.12 • A.13 • A.14 • A.16 • Annex A additional ISO 27017, 27018, and ISO 27701 implementation guidance • 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.8.1 • CLD.9.5.1 • CLD.9.5.2 • CLD.12.1 • CLD.12.4 • CLD.13.1 • ISO 27018 extended control set for PII protection (A02-A12) • Sampled ISO 27701 Annex B Control Testing for PII Processors • B.8.3 • B.8.5	Redmond, WA, and Sampled Data Centers	10 days remote 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 framework (clauses 4-10) - Annex A (A5-A18) - Annex A additional ISO 27017, ISO 27018, and ISO 27701 implementation guidance - Site-specific Annex A controls for locations to be assessed - 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)	Redmond, WA, and Sampled Data Centers	13.0 on-site days / 5.0 days planning and reporting	March – April 2023

▨ 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 Applied AI Services	✓	✓
	Azure Bot Service	✓	✓
	Azure Open Datasets	✓	-
	Cognitive Services	✓	✓
	Cognitive Services: Anomaly Detector	✓	-
	Cognitive Services: Form Recognizer	✓	✓
	Cognitive Services: Metrics Advisor	✓	-
	Cognitive Services: Computer Vision	✓	✓
	Cognitive Services: Container Platform	✓	✓
	Cognitive Services: Content Moderator	✓	✓
	Cognitive Services: Custom Vision	✓	✓
	Cognitive Services: Cognitive Service Platform	✓	✓
	Cognitive Services: Face	✓	✓
	Cognitive Services: Immersive Reader	✓	-
	Cognitive Services: Personalizer	✓	✓
	Cognitive Services: Text Analytics	✓	✓
	Cognitive Services: Language Understanding	✓	✓

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
AI + Machine Learning	Cognitive Services: Translator	✓	✓
	Cognitive Services: QnAMaker Service	✓	✓
	Cognitive Services: Speech Services	✓	✓
	Cognitive Services: Video Indexer	✓	✓
	Azure Machine Learning	✓	✓
	AI builder	✓	✓
	Machine Learning Studio (Classic)	✓	-
	Microsoft Genomics	✓	-
	Microsoft Autonomous Development Platform	✓	-
	Azure Health Bot	✓	-
Analytics	Azure Analysis Services	✓	✓
	Azure Data Explorer	✓	✓
	Data Factory	✓	✓
	HDInsight	✓	✓
	Azure Stream Analytics	✓	✓
	Data Catalog	✓	-
	Data Lake Analytics	✓	-
	Azure Data Share	✓	✓
	Power BI Embedded	✓	✓
Compute	Cloud Services	✓	✓
	Azure Service Fabric	✓	✓
	Virtual Machine Scale Sets	✓	✓
	Virtual Machines	✓	✓
	Batch	✓	✓
	Azure Functions	✓	✓
	App Service	✓	✓
	App Service – Web Apps (including Containers)	✓	✓
	App Service – API Apps	✓	✓
	App Service – Mobile Apps	✓	✓
	App Service -Static Web Apps	✓	✓
	Guest Configuration	✓	✓

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
Compute	Azure Vmware Solution	✓	-
	Planned Maintenance	✓	✓
	Azure Arc-enabled Servers	✓	✓
	Azure VM Image Builder	✓	-
	Azure Virtual Desktop	✓	✓
	Azure Service Manager (RDFE)	✓	✓
Containers	Azure Kubernetes Service (AKS)	✓	✓
	Azure Arc enabled Kubernetes	✓	✓
	Azure Kubernetes Configuration Management	✓	✓
	Azure Red Hat OpenShift (ARO)	✓	-
	Container Instances	✓	✓
	Container Registry	✓	✓
	Azure Container Service	✓	✓
Databases	Azure Cosmos DB	✓	✓
	Azure SQL	✓	✓
	Azure Database for MariaDB	✓	✓
	Azure Database for MySQL	✓	✓
	Azure Database for PostgreSQL	✓	✓
	Azure Database Migration Service	✓	✓
	Azure Cache for Redis	✓	✓
	Azure Health Data Services (formerly Azure API for FHIR)	✓	✓
	Azure Synapse Analytics	✓	✓
	SQL Server Registry	✓	-
	SQL Server Stretch Database	✓	✓
	Azure SQL Database Edge	✓	-
	Azure Managed Instance for Apache Cassandra	✓	-
Developer Tools	Azure DevTest Labs	✓	✓
	Azure Lab Services	✓	✓
	Azure for Education	✓	-
	Application Change Analysis	✓	-
	Azure App Configuration	✓	✓

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
Developer Tools	GitHub AE	✓	✓
Identity	Azure Information Protection	✓	✓
	Azure Active Directory (Free, Basic, Premium)	✓	✓
	Microsoft Accounts	✓	-
	Azure Active Directory B2C	✓	✓
	Azure Active Directory Domain Services	✓	✓
Integration	Logic Apps	✓	✓
	API Management	✓	✓
	Service Bus	✓	✓
Internet of Things	Event Hubs	✓	✓
	Event Grid	✓	✓
	Azure IoT Central	✓	-
	Azure IoT Hub	✓	✓
	Notification Hubs	✓	✓
	Azure Sphere	✓	✓
	Azure Time Series Insights	✓	-
	Windows 10 IoT Core Services	✓	-
	Logic Apps	✓	✓
	API Management	✓	✓
	Microsoft Azure Peering Service	✓	✓
	Azure Defender for IoT	✓	✓
	Azure Digital Twins	✓	-
	Microsoft Cloud for Sustainability	✓	-
Management and Governance	Application Change Analysis	✓	-
	Azure Resource Manager (ARM)	✓	✓
	Automation	✓	✓
	Azure Advisor	✓	✓
	Azure Lighthouse	✓	✓
	Azure Managed Applications	✓	✓
	Azure Migrate	✓	✓
	Azure Monitor	✓	✓

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
Management and Governance	Azure Policy	✓	✓
	Azure Resource Graph	✓	✓
	Cloud Shell	✓	✓
	Microsoft Azure Portal	✓	✓
	Azure Blueprints	✓	-
	Scheduler	✓	✓
	Cost Management	✓	✓
	Azure Signup Portal	✓	✓
	Resource Move	✓	-
	Quota+ Usage blade	✓	✓
	Microsoft Purview (formerly Azure Purview)	✓	-
Media	Azure Media Services	✓	✓
Mixed Reality	Azure Spatial Anchors	✓	-
	Azure Remote Rendering	✓	-
Networking	Application Gateway	✓	✓
	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 Web Application Firewall	✓	✓
	Content Delivery Network	✓	✓
	Network Watcher	✓	✓

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
Networking	Traffic Manager	✓	✓
	Virtual WAN	✓	✓
	Azure Public IP	✓	✓
	Virtual Network NAT	✓	✓
	Azure Route Server	✓	✓
Security	Key Vault	✓	✓
	Azure Payment HSM	✓	-
	Multi-Factor Authentication	✓	✓
	Azure Dedicated HSM	✓	✓
	Customer Lockbox for Microsoft Azure	✓	✓
	Microsoft Sentinel (formerly Azure Sentinel)	✓	✓
	Microsoft Defender for Cloud (formerly Security Center)	✓	✓
	Microsoft Azure Attestation	✓	-
	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 Archive Storage	✓	✓
	Azure Import/Export	✓	✓
	Azure Data Box	✓	✓
	Azure HPC Cache	✓	✓
	Azure Site Recovery	✓	✓
	StorSimple	✓	✓
	Azure Backup	✓	✓
	Azure File Sync	✓	✓
	Azure NetApp Files	✓	✓
	Azure Data Lake Storage Gen 1	✓	-
Web	Azure Cognitive Search	✓	✓
	Azure Maps	✓	✓
	Azure SignalR Service	✓	✓
	Azure Web PubSub	✓	✓
	Azure Spring Cloud Service	✓	-

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
Supporting Infrastructure and Platform Services		✓	✓
Microsoft Online Services			
Appsource		✓	-
Intelligent Recommendations		✓	-
Microsoft Intune		✓	✓
Microsoft Defender for Cloud Apps		✓	✓
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		✓	✓
Dynamic 365 Customer Voice		✓	✓
Microsoft Bing for Commerce		✓	-
Universal Print		✓	-
Update Compliance		✓	-
Microsoft Dynamics 365			
Dynamics 365 Customer Service		✓	✓
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		✓	-

Product Category	Service/Offering Name	Cloud Environment Scope	
		Azure	Azure Government
	Dynamics 365 Finance	✓	✓
	Dynamics 365 Fraud Protection	✓	-
	Dynamics 365 Marketing	✓	-
	Power Pages (formally Power Apps 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	✓	-
	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	✓	-
	Dynamics 365 Business Q&A	✓	-
	Dynamics 365 Talent Attract & Onboard	✓	-
	Dynamics 365 Customer Service Insights	✓	-
	Dynamics 365 Remote Assist	✓	✓
	Business 360 AI Platform	✓	-
	Dataverse	✓	✓
Microsoft Cloud for Financial Services			
	Unified Customer Profile	✓	-
	Collaboration Manager	✓	-
	Customer Onboarding	✓	-

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 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 datacenters in scope for the purposes of this report are:

The datacenters within scope of the IMS are as follows:

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 (SJC20/21/22/31)
West US 2	Quincy, WA (CO1/2/6, MWH01/02/03/04/05/20/21)
West US 3	Phoenix, AZ (PHX10/70/80)
West Central US	Cheyenne, WY (CYS01/04/05/08)
Central US	Des Moines, IA (DM1/2/3/4, DSM05/06/07/08/09/10)
North Central US	Chicago, IL (CH1/2/4, CHI20/21/23/25)
South Central US	San Antonio, TX (SN1/2/3/4/6/7, SAT09/10/11/20)
East US	Bristow, VA (BLU) Reston, VA (BL4) Sterling, VA (BL20) Ashburn, VA (BL2/3/5/6/7/21/22/23/24/30/31) Manassas, VA (MNZ20/22) Dulles, VA (IAD01/20)
East US 2	Boydton, VA (BN1/3/4/6/7/8/9/10/13/14, LVL01/02)
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 (YTO20/21/22/23/24)
Brazil South	Campinas, Brazil (CPQ01/02/20/21/22/23/24) Sao Paulo, Brazil (GRU)
Brazil Southeast	Rio de Janeiro, Brazil (RIO01/20)

Microsoft Azure International Datacenters	
West Europe	Amsterdam, Netherlands (AM3, AMS04/05/06/07/08/09/11/12/20/21/22/23/24)
North Europe	Dublin, Ireland (DB3/4/5, DUB06/07/08/09/10/12/13/20/21/24/31)
UK South	London, United Kingdom (LON21/22/23/24/25/26/28)
UK West	Cardiff, United Kingdom (CWL20)
France Central	Paris, France (PAR20/21/22/23/24)
France South	Marseille, France (MRS20/21)
Germany North	Berlin, Germany (BER20/21)
Germany Northeast	Leipzig-Halle, Germany (LEJ20)
Germany West Central	Frankfurt, Germany (FRA21/22/23)
Germany Central	Frankfurt, Germany (FRA20)
Sweden Central	Gavleborg, Sweden (GVX01/11/21)
Switzerland West	Geneva, Switzerland (GVA20)
Switzerland North	Zurich, Switzerland (ZRH20/22)
East Asia	Hong Kong (HK2, HKG20/21/22/23)
Southeast Asia	Singapore (SG2/3, SIN20/21/22)
West India	Mumbai, India (BOM01)
Central India	Dighi, India (PNQ01/20/21/22)
South India	Ambattur, India (MAA01, MAA20)
Jio India Central	Nagpur, India (NAG20)
Jio India West	Jamnagar, India (JGA20)
Japan West	Osaka, Japan (OSA01/02/20/21/22)
Japan East	Tokyo, Japan (TYO01/20/21/22/23/31)
Korea South	Busan, South Korea (PUS04/20)
Korea Central	Seoul, South Korea (SEL20/21/22)
UAE Central	Abu Dhabi (AUH20)
UAE North	Dubai (DXB20/21/22/23)
Australia East	Macquarie Park, Australia (SYD03) Sydney, Australia (SYD21/22/23/24/25/26/27)
Australia Southeast	Melbourne, Australia (MEL01/20/21/23/24)
Australia Central	Canberra, Australia (CBR20/22)
Australia Central 2	Canberra, Australia (CBR21/23)
South Africa North	Johannesburg, South Africa (JNB20/21/22/23)
South Africa West	Cape Town, South Africa (CPT20)
Norway East	Oslo, Norway (OSL20/21/22/23/24)
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)	Marseille, France (MRS01)
Athens, Greece (ATH01)	Memphis, TN (MEM30)
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)	Nashville, TN (BNA30)
Bucharest, Romania (BUH01)	New Delhi, India (DEL01)
Budapest, Hungary (BUD01)	New York City, NY (NYC)
Buenos Aires, Argentina (BUE30)	Newark, NJ (EWR30)
Busan, South Korea (PUS03)	Osaka, Japan (OSA30/31)
Cape Town, South Africa (CPT02)	Oslo, Norway (OSL30)
Cairo, Egypt (CAI30)	Palo Alto, CA (PAO)
Chennai, India (MAA02)	Paris, France (PAR02/PRA)
Chicago, IL (CHG/CHI30)	Perth, Australia (PER01/30)
Copenhagen, Denmark (CPH30)	Philadelphia, PA (PHL30)
Dallas, TX (DAL, DFW30)	Phoenix, AZ (PHX31)
Denver, CO (DNA)	Portland, OR (PDX31)
Detroit, MI (DTT30)	Prague, Czech Republic (PRG01)
Dubai, United Arab Emirates (DXB30)	Queretaro, Mexico (MEX30/31)
Dusseldorf, Germany (DUS30)	Rabat, Morocco (RBA30)
Frankfurt, Germany (FRA/FRA31)	Rio De Janeiro, Brazil (RIO02/03)
Geneva, Switzerland (GVA30)	Rome, Italy (ROM30)
Helsinki, Finland (HEL03)	Salt Lake City, UT (SLC31)

Edge Sites	
Ho Chi Minh, Vietnam (SGN30)	Sao Paulo, Brazil (SAO03/31)
Hong Kong (HKB, HKG30)	San Diego, California (SAN30)
Honolulu, HI (HNL01)	San Jose, CA (SJC)
Houston, TX (HOU01)	Santiago, Chile (SCL30)
Hyderabad, India (HYD30)	Seattle, WA (STB)
Istanbul, Turkey (IST30)	Seoul, South Korea (SLA)
Jacksonville, FL (JAX30)	Singapore (SGE, SG1, SIN30)
Jakarta, Indonesia (JKT30)	Sofia, Bulgaria (SOF01)
Johannesburg, South Africa (JNB02)	Stockholm, Sweden (STO)
Kiev, Ukraine (IEV30)	Taipei, Taiwan (TPE30/31)
Kuala Lumpur, Malaysia (KUL01/02/30)	Tampa, FL (TPA30)
Las Vegas, NV (LAS01/30)	Tel Aviv, Israel (TLV30)
Lisbon, Portugal (LIS01)	Tokyo, Japan (TYA/TYB)
Los Angeles, CA (LAX, LAX31)	Toronto, Canada (YTO01/30)
Lagos, Nigeria (LOS30)	Vancouver, Canada (YVR30)
London, United Kingdom (LON04/LTS)	Warsaw, Poland (WAW01)
Madrid, Spain (MAD30)	Zagreb, Croatia (ZAG30)
Manchester, United Kingdom (MAN30)	Zurich, Switzerland (ZRH)
Manila, Philippines (MNL30)	

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.