# MICROSOFT AZURE, DYNAMICS 365, AND ONLINE SERVICES

## ISO/IEC 20000-1:2018 CERTIFICATION - RECERTIFICATION REVIEW SUMMARY REPORT

APRIL 24, 2023

Assessment and Compliance Services

## Statement of Confidentiality

The sole purpose of this document is to provide Microsoft Corporation (Microsoft) with the summary of the ISO/IEC 20000-1:2018 (ISO 20000-1) recertification 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 20000-1 recertification 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 Service Management System (SMS) 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 20000-1. 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/IEC 27001:2022 recertification review
- ISO 9001:2015 recertification review
- ISO 22301:2019 recertification review
- Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) certification review

# Table of Contents

# SECTION I

## AUDIT TEAM RECOMMENDATION

# Audit Team Recommendation, and General Design and Operating Effectiveness of the SMS

**Summary of Findings and Recommendation, General Design and Operating Effectiveness of the Client SMS**

Overall, the SMS appears to be operating effectively and the client has met the requirements of the ISO 20000-1 standard. There were no nonconformities noted as a result of the 2023 recertification review.

Microsoft Azure, Dynamics, and other Online Services (Microsoft Azure) has implemented and maintains policies and procedures that are designed in accordance with the ISO 20000-1 standard. The policies are well-defined, detailed, regularly reviewed and updated, communicated, and understood by users within the organization. This includes both Microsoft corporate level and Microsoft Azure, Dynamics and other Online Services policies and procedures which have been adopted to support the implementation of the SMS. Microsoft Azure, Dynamics, and other Online Services has defined standard operating procedures (SOPs) at a team level to provide additional guidance to personnel.

The audit team concluded that procedures were effectively implemented within the organization to monitor conformance with the standard and achievement of objectives specified by Microsoft Azure that are in alignment with the strategic direction of the organization. Based on the activities demonstrated by Microsoft Azure management and the supporting documentation provided during the course of the recertification review, the audit team determined that effective processes were in place to manage and monitor information security risks and to identify and monitor compliance with relevant standards and contractual commitments. The Microsoft Azure leadership team has supported the SMS by providing the resources necessary to maintain and implement risk treatment plans and projects designed to improve the risk posture of the organization.

A formally defined global risk management program is in place, and Microsoft Azure has demonstrated an effective process to manage and monitor risk in accordance with the direction of management and the organization's tolerance for risk. The sponsorship of the SMS is headed by the Integrated Management Forum (IMF). The IMF is the management group that oversees the various components of the SMS and the communication and exchange of information between those components.

It is the audit team's recommendation to re-issue the certification for another three-year term and reflecting the updated scope statement.

| Finding Ref | Status | Correction[1] | Corrective Action Plan[1] | Evidence of Remediation[1] |
|---|---|---|---|---|
| No nonconformities were identified during the 2023 recertification 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 SMS was appropriate, and the audit objectives of the recertification review were met.

| Clause | Conclusion | Comment |
|---|---|---|
| Context of the Organization – Understanding the Organization and its Context | Effective | No Comment |
| Context of the Organization – Understanding the Needs and Expectations of Interested Parties | Effective | No Comment |
| Context of the Organization – Determining the Scope of the Service Management System | Effective | No Comment |
| Context of the Organization –Service Management System | Effective | No Comment |
| Leadership – Leadership and Commitment | Effective | No Comment |

| Clause | Conclusion | Comment |
|---|---|---|
| Leadership – Policy | Effective | No Comment |
| Leadership – Establishing the Service Management Policy | Effective | No Comment |
| Leadership – Communicating the Service Management Policy | Effective | No Comment |
| Leadership – Organizational Roles, Responsibilities and Authorities | Effective | No Comment |
| Planning – Actions to Address Risks and Opportunities | Effective | No Comment |
| Planning – Service Management Objectives and Planning to Achieve Them | Effective | No Comment |
| Planning – Plan the Service Management System | Effective | No Comment |
| Support of the Service Management System – Resources | Effective | No Comment |
| Support of the Service Management System – Competence | Effective | No Comment |
| Support of the Service Management System – Awareness | Effective | No Comment |
| Support of the Service Management System – Communication | Effective | No Comment |
| Support of the Service Management System – Documented Information | Effective | No Comment |
| Support of the Service Management System - Knowledge | Effective | No Comment |
| Operation of the Service Management System – Operational Planning and Control | Effective | No Comment |
| Operation of the Service Management System – Service Portfolio | Effective | No Comment |
| Operation of the Service Management System – Relationship and Agreement | Effective | No Comment |
| Operation of the Service Management System – Supply and Demand | Effective | No Comment |
| Operation of the Service Management System – Service Design, Build and Transition | Effective | No Comment |
| Operation of the Service Management System – Resolution and Fulfilment | Effective | No Comment |
| Operation of the Service Management System – Service Assurance | Effective | No Comment |
| Performance Evaluation – Monitoring, Measurement, Analysis and Evaluation | Effective | No Comment |
| Performance Evaluation – Internal Audit | Effective | No Comment |
| Performance Evaluation – Management Review | Effective | No Comment |
| Performance Evaluation – Service Reporting | Effective | No Comment |
| Improvement – Nonconformity / Corrective Action | Effective | No Comment |
| Improvement – Continual Improvement | Effective | No Comment |

**Performance of the SMS Over the Certification Cycle**

Overall, Microsoft continued to demonstrate a sound understanding of its SMS as it continued to meet the requirements of the ISO 20000-1 standard. During the recertification review, an assessment was performed to

determine the overall effectiveness of the SMS during the certification lifecycle and no negative trends were identified. The SMS 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. During the previous certification term, Microsoft continued to expand their SMS scope to include additional service offerings and data center locations, and did so in continued conformance of the ISO 20000-1 standard and with regard to achieving the objectives of Microsoft's service management policy and Microsoft's maintenance, monitoring, and improvement activities of the SMS.

Microsoft has implemented continual improvement activities since the 2022 surveillance 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 with the client obligations and marketing guidelines provided to Microsoft.

# SECTION 2

## PROJECT OVERVIEW

# EXECUTIVE SUMMARY

### Introduction

Microsoft (or the "client") was the subject of a recertification review from February to April 2023 of their ISO 20000-1 (or the "standard") certification which was originally issued in June 2020. The purpose of the recertification review was to verify that the approved SMS continued to be effectively 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. This report includes the results of the 2023 recertification review mentioned above.

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

- The system 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 SMS standard ISO 20000-1 and other documents required for certification
- Changes to the documented system
- Areas subject to change
- Selected elements of ISO 20000-1
- Assessment of the management system over the course of the certification lifecycle
- Other selected areas as appropriate

The scope of the review was limited to the SMS supporting Microsoft Azure, Dynamics, 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. The scope of the SMS includes the SMS 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. 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 04:00 PM PST on Tuesday, February 7, 2023. The meeting was held to kick-off the recertification activities. An agenda was provided as well as a project plan and audit plan for the recertification review. The opening meeting was held to perform the following:

- Reconfirm the audit plan, scope, and deliverables for the recertification 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 recertification audit covered the documentation requirements of the ISO 20000-1 standard, as well as testing which included evidence of the monitoring, maintenance, and operating effectiveness of the SMS. The recertification audit objectives included the following:

- Determine the continued conformance of the SMS to the ISO 20000-1 standard, specifically with regard to achieving the objectives of Microsoft's service management policy and Microsoft's maintenance, monitoring, and improvement activities of the SMS.
- Determine the effectiveness of the procedures and processes for evaluation and review of compliance with relevant legislation and regulations.
- Validate the functions at each in-scope location to help ensure the functions performed are relevant to the scope of the management system.
- Review the performance of the management system over the period of certification, including the review of previous surveillance audits.

The focus of the review enabled Schellman to maintain confidence that Microsoft's certified SMS continued to fulfill the requirements of ISO 20000-1 between recertification audits. The ISO 20000-1 recertification included an analysis of the following SMS activities, as applicable:

- assessment of monitoring, measurement, analysis, and evaluation to ensure that the methods selected produce comparable and reproducible results;
- documentation information required per clauses 4 through 10 of ISO 20000-1;
- reviews of the effectiveness of the SMS and measurements of the effectiveness of the service controls, reporting, and reviewing against the SMS objectives;
- internal audits and management reviews;
- management responsibility for the service management policy;
- leadership and support of the SMS;
- implementation of controls, taking into account the organization's measurements of effectiveness of controls, to determine whether controls are implemented and effective to achieve the stated objectives;
- programs, processes, procedures, records, internal audits, and reviews of the SMS effectiveness to ensure that these are traceable to management decisions and the SMS policy and objectives;
- whether the SMS documents information required by ISO 20000-1 and information determined by the organization as being necessary for the effectiveness of the SMS;
- complaints handling;
- progress of planned activities aimed at continual improvement;
- continuing operational control;
- review of any changes as well as an assessment of the certification lifecycle;
- use or marks and/or any reference to certification; and
- the performance of the management system over the period of certification, including the review of previous surveillance audits.

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

A closing meeting occurred remotely utilizing the Microsoft Teams web conferencing application, at approximately 4:00 PM PST on Monday, April 24, 2023. The closing meeting included discussions on the conformity of the client's SMS in relation to the ISO 20000-1 standard and discussions regarding the recommendation to reissue the certificate of conformance.

**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.

# SMS Review

**Context of the Organization (Clause 4)**

Understanding the Organization and its Context (Clause 4.1)

Microsoft Azure management recognizes the need to deliver services of an agreed quality to its customers and therefore, has established a SMS in accordance with the ISO 20000-1 standard, which includes consideration of applicable statutory, regulatory, and contractual information security requirements. The SMS has been established as part of Microsoft's IMS, which also includes the information security management system (ISMS), privacy information management system (PIMS), business continuity management system (BCMS), and quality management system (QMS). As such, Microsoft Azure management has considered internal and external issues relevant to security, privacy, business continuity, quality, and service management.

Microsoft Azure management have accounted for the following internal and external issues as part of the SMS manual.

Understanding the Needs and Expectations of Interested Parties (Clause 4.2)

Microsoft Azure considers input from the relevant interested parties to determine the obligations and expectations that Microsoft Azure needs to meet. Microsoft Azure management engages with the relevant interested party, on a periodic basis, to discuss the requirements and align Microsoft Azure's plans. The relevant interested parties that provide input to the SMS are defined in the SMS manual.

Determining the Scope of the ISMS (Clause 4.3)

The scope of the SMS is defined and documented as part of the IMS scope statement, which was most recently updated as of April 14, 2023, version 2023.03. The scope of the SMS is reviewed by the Microsoft compliance manager at least annually or upon significant changes.

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

Service Management System (Clause 4.4)

Microsoft has established an IMS scope statement which serves as a framework to lead the implementation, maintenance, and continual improvement of the SMS in accordance with the requirements of the standard. 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.

Management is committed to establishing, implementing, maintaining, and continually improving the SMS, which includes the processes needed and their interactions, in accordance with the requirements of ISO 20000-1. The plan, do, check, act approach has been implemented to help ensure that processes, products, and services within scope of the SMS are continually improved.

**Leadership (Clause 5)**

Leadership and Commitment and Organizational Roles, Responsibilities and Authorities (Clause 5.1 and 5.3)

*Leadership and Commitment*

Microsoft is committed to ensuring the confidentiality, integrity, and availability (CIA) of information through the appropriate application of people, process, organization, and technology complying with applicable regulatory standards and contractual requirements. Information assets must be protected from threats identified, whether internal or external, deliberate, or accidental.

Microsoft Azure leadership's responsibility and commitment to SMS is demonstrated by creating and maintaining this SMS, providing customer support and other resources to support the provision of services, defining online service terms (OST) and service level agreements (SLAs) for services, and providing open communication with customers and service teams on the health and provision of services within the scope of the services provided by the Microsoft Azure, Dynamics, and Online Services.

*Organizational Roles, Responsibilities and Authority*

Organizational roles, responsibilities, and authorities relevant to the SMS have been established as part of the IMS manual and the SMS manual. Organizational charts are also in place to define the organizational structure, reporting lines, and authorities. These charts are communicated to employees and updated as needed.

The IMF has been established to oversee the various components of the IMS, including the communication and exchange of information between those components. The objective of the IMF is to help ensure the operating effectiveness and continual improvement of the SMS.

Assignees have been appointed to the IMF and delegated the following roles and responsibilities as part of the SMS manual. The IMF's role is to provide management oversight and guidance on the business operations and effectiveness of the SMS via periodic meetings. The cadence for the review is summarized within the management review section below.

Policy (Clause 5.2)

Top management is committed to fulfilling the service requirements made to Microsoft Azure, Dynamics, and Online Services customers as outlined in their corresponding terms, service level agreements, and / or subscription agreements. The aforementioned documents are made available to customers as part of Microsoft's external facing website. To help meet the aforementioned service requirements, a suite of supporting information security policies has been established.

The IMF is responsible for establishing information security policies that are appropriate for the purpose of the organization and provide a framework for setting service management objectives. This includes ensuring that information security policies align with operational, legal and / or regulatory requirements.

Information security policies are documented, communicated to the Microsoft workforce, and available to interested parties, as appropriate. More specifically, information security policies are communicated internally via SharePoint site. Information security policies are also reviewed for appropriateness at least annually, or more often as needed.

## Planning (Clause 6)

Actions to Address Risks and Opportunities (Clause 6.1)

Microsoft Azure Global risk management program (RMP) is in place to oversee and evaluate existing and emerging risks / threats to Microsoft Azure environment. The RMP aligns the risk management framework with the Microsoft Azure risk management procedures and processes (Microsoft Azure engineering, service operation, infrastructure, and compliance). This includes determining relevant external and internal issues that impact and affect the outcome of the SMS.

*Risk Assessment*

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 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.

*Risk Treatment*

The Microsoft enterprise risk management office (RMO) establishes risk treatment plans based on inherent risk and control effectiveness criteria.

Microsoft Azure security and engineering teams are responsible and accountable to work in conjunction with the risk manager to identify and prioritize the remediation of the risks tagged as important. These risks / work items are tracked via internal tools for closure and monitored by leadership, as appropriate.

The most recent information security risk assessment and risk treatment processes took place during the first half of Microsoft's 2023 fiscal year. The results of the risk assessment and the status of risk treatment plans were reviewed on October 10, 2022, as a component of the semi-annual enterprise risk discussion.

Service Management Objectives and Planning to Achieve Them (Clause 6.2)

Microsoft has established relevant service management objectives at appropriate and relevant functions and levels to help ensure that mechanisms are in place for planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the SMS. These objectives are established in-line with the strategic direction of Microsoft Azure.

The leadership team has established appropriate forums to discuss the key performance indicators, prioritize and monitor progress, and provide input for continual improvement.

Plan the Service Management System (Clause 6.3)

Microsoft Azure, Dynamics, and Online Services management is committed to continual improvement of the effectiveness of the SMS through the use of the information security policy, control objectives, audit results, analysis of monitored events, along with corrective and preventive actions and management reviews. Microsoft Azure retains documentation per the document and record management SOP.

**Support (Clause 7)**

Resources (Clause 7.1)

Top management is committed to the effectiveness and continual improvement of the SMS. Periodic reviews are scheduled to allocate appropriate resources to meet operational requirements and implement corresponding action for improving the effectiveness of the SMS and to enhance customer satisfaction. Through the periodic IMF meetings, management provides guidance, resources, budget, and planning to successfully meet the service management objectives.

Competence, Awareness, and Knowledge (Clauses 7.2, 7.3, and 7.6)

Prior to employment, employees are put through a screening process, which limits employment to qualified candidates (based on education, experience, training etc.). The HR screening process is continuously reviewed and updated to provide reasonable assurance that only competent employees are hired.

Microsoft full-time employees (FTEs) and contingent staff are required to undergo mandatory training on at least an annual basis. Training includes security foundations training and / or role-based training to help ensure competency for their relevant job function and awareness around general information security best practices. New hires are required to take mandatory training before accessing the system or performing assigned duties and suppliers are required to complete supplier code of conduct training upon hire. Additional security awareness campaigns are also made available to FTEs and contingent staff, whereas the required frequency of training is dependent on the user's job title and / or role. Periodic brown bag training sessions, seminars, and training sessions may also be provided to help supplement further development and competency.

Communication (Clause 7.4)

Microsoft Azure, Dynamics, and Online Services management is committed to proper communication with the internal and external stakeholders regarding the state of the SMS. 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 IMS communication plan. The IMS communication plan is reviewed at least annually or as needed for appropriateness.

Documented information (Clause 7.5)

Microsoft has established requirements for documented information as part of the SMS manual and document and record management SOP to help ensure effective planning, operation, and control of the SMS. The SOP is applied to all documents and records related to the SMS, regardless of whether the documents and records were created internally or whether they are of external origin. The policy encompasses all documents and records stored in any format (e.g., paper, audio, video, etc.).

Documents are reviewed and approved at least annually or upon significant change. Documents are distributed and protected via the internal SharePoint portal that is shared with employees. The portal is protected by access and authentication controls. Only authorized users are provided with write-access. Other users have view / read-only rights by default. When documents are no longer required, they are disposed of according to secure disposal practices.

The SMS defines documented information required by the ISO 20000-1 standard and necessary for the effectiveness of the SMS.

**Operation (Clause 8)**

Operational Planning and Control (Clause 8.1)

The SDL SOP establishes the SDL process and minimum set of procedures to ensure that the high security standard is maintained for Microsoft Azure products and services development. The service teams follow the SDL process for secure software release management.

Service Portfolio (Clause 8.2)

*Service Delivery and Service Catalogue Management*

Microsoft Azure, Dynamics, and Online Services maintains a service portfolio to help manage the entire service lifecycle, including proposed services, services in development, services in production, and services that are to be removed. An external facing products catalogue is made available to interested parties that includes an overview of products and services, the intended outcomes of products and services, and third-party integrations. Services to be provided to customers are agreed upon within the Microsoft Azure, Dynamics, and Online Services management portal as part of external facing OSTs and other agreements. SLAs are also communicated to customers within the Azure, Dynamics, and Online Services dashboard that is made available to customers via the Azure, Dynamics, and Online Services management portal.

*Plan the Services*

Microsoft Azure, Dynamics, and Online Services management has established a process to plan and onboard new services before they become generally available to customers. Services are assessed against Microsoft Azure, Dynamics, and Online Services' objectives, security requirements, privacy requirements, SOPs, policies, and processes prior to becoming generally available.

*Control of Service Lifecycle Parties*

Microsoft has established a SSPA program which sets privacy and security requirements for Microsoft suppliers and maps its compliance requirement to the security requirements. The SSPA program is a partnership between Microsoft procurement, CELA, and corporate security. These partners develop and contribute to the supplier requirements to ensure that privacy and security principles are followed when suppliers handle Microsoft Azure personal or confidential data. Microsoft Azure uses service providers in a variety of roles across the different functions and business units and manages the service providers through the supplier management program and Microsoft security policy which includes governance and oversight mechanisms operated by other parties.

Based on the services to be provided, the Microsoft Azure, Dynamics, and Online Services managers are responsible for ensuring that the contract with the third-party service provider includes appropriate information exchange agreements on confidentiality, privacy, and security requirements, including the use of non-disclosure agreements (NDAs). The third-party management SOP provides additional details surrounding the supplier relationship management process.

*Asset Management and Configuration Management*

Asset management procedures have been established to help ensure that assets used to deliver services are managed to meet service requirements and obligations. The asset management SOP defines guidelines to help ensure that assets are handled securely and provided with an appropriate level of protection as per their classification. The asset owner, classification, location, purpose, and retention must be defined for each asset. Asset owners are ultimately accountable for the CIA of their assets.

Relationship and Agreement (Clause 8.3)

Microsoft Azure, Dynamics, and Online Services may use external suppliers, internal suppliers, or customers acting as a supplier to meet the following service requirements:

- provide or operate services;
- provide or operate service components; or
- operate processes, or parts of processes that are in the organization's SMS.

*Service Level Management*

A list of products and services is maintained and communicated to customers as part of the external facing products catalogue, which contains an overview of products and service offerings, in addition to other Microsoft or third-party tools for which the specific service is integrated with. SLAs are also maintained and communicated to customers for the services to be provided as part of the Microsoft Azure, Dynamics, and Online Services management portal.

*Supplier Management*

Microsoft has defined the SSPA program to help ensure that suppliers are managed in alignment with Microsoft's security, privacy, and compliance requirements. The SSPA program and MSPP dictate where a third-party can access, process, host or manage assets supporting Microsoft Azure, Dynamics, and Online Services. Arrangements are made in a formal contract to define responsibility and requirements for the security and CIA of the information assets involved. Appropriate security standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the MSPP.

The third-party management SOP states that each Microsoft Azure, Dynamics, and Online Services team is responsible for managing its own third-party relationships, including contract management, monitoring metrics (e.g., SLAs) and third-party access to systems. This SOP also outlines the procedures for hiring third-party service providers.

Supply and Demand (Clause 8.4)

*Budgeting and Accounting for Services*

Microsoft management is committed to continual improvement and effectiveness of the SMS. 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.

*Demand Management and Capacity Management*

A capacity management program has been established to help achieve the following Microsoft Azure, Dynamics, and Online Services demand and capacity management requirements.

Capacity planning is discussed as part of quarterly CAI fundamental reviews and twice a year during the semester greenlight meetings. Capacity-related reports are communicated to customers via the Trust Portal.

Service Design, Build and Transition (Clause 8.5)

Microsoft has established a suite of change management policies and procedures to define service components and other items that are under the control of change management, categories of change and how they are managed, and criteria to determine changes with the potential to have a major impact on customers or services. Change management policies and procedures include but are not limited to the software change and release management SOP, configuration management SOP, and SDL SOP, and are made available to relevant personnel and interested parties via the internal SharePoint site. SOPs are reviewed at least annually by the required stakeholders.

The software change and release management process are used to plan, schedule, develop, approve, apply, distribute, and track software changes to production to help ensure the integrity and reliability of the environment while meeting customer expectations. As per the software change and release management SOP, all change management procedures must be documented, approved, and maintained. The SOP outlines the six phases of product planning, engineering planning, development, release management, deployment, and live site support. Software changes are initiated at the product planning phase, at which time business goals, priorities and scenarios are identified and agreed upon. The engineering planning phase defines the scenarios identified through detailed requirements documents, design documents, operational planning, and test plans when applicable.

Software change releases are broadly categorized as a major change release, minor change release, or revision change release. Change type is used to help determine the appropriate documentation, handling, testing, and approval requirements prior to release and deployment. The addition of new services and / or major functionality changes are considered major changes and therefore have the potential to have a major impact on customers or

services. Changes that have a major impact to services offered to customers are assessed via privacy reviews and the SDL process. Critical security reviews and approval checkpoints are also included in the SDL process.

Resolution and Fulfilment (Clause 8.6)

*Incident and Service Request Management*

Microsoft Azure has established a formal SOP for incident management that defines the organization's approach for managing and resolving incidents related to the cloud and artificial intelligence services. The SOP establishes the minimum baseline set of procedures for cloud service engineering and operations teams for managing incidents and responding to them appropriately. The incident response team establishes incident response policies and procedures. These policies and procedures address the recording, prioritization, classification, updating of records, escalation, resolution, closure and required coordination among the teams that support event and incident response for the environment and physical infrastructure.

*Problem Management*

As part of the incident management process, incidents are assessed as problems and require a root cause analysis through a post incident review (PIR). A PIR is documented for a customer impacting incident event triggering commitments in the SLAs. Lessons learnt related to the incident response process is documented. Detailed incident handling procedures are documented in the incident management SOP.

Additionally, incidents are reviewed through several meetings including greenlight (i.e., planning), IMS review, and CE fundamentals for trend analysis of incidents and the effectiveness of the resolution of incidents.

Service Assurance (Clause 8.7)

*Service Availability Management*

A dedicated risk management program is in place to oversee and evaluate the existing and emerging risks / threats to the Microsoft Azure, Dynamics, and Online Services environment, including the risks to service continuity and availability.

Service continuity and availability requirements including access rights, service response times, and end-to-end availability of services are agreed with customers via the OST during subscription of the service.

*Service Continuity Management*

Microsoft Azure has documented a process to develop service continuity and availability plans as part of the business continuity (BC) and DR SOP. The BC and DR SOP define procedures for the development of availability targets and recovery requirements as part of the business impact assessment (BIA). The MSPP also defines policy objectives for the establishment and maintenance of a BC management program (BCMP) for Microsoft Azure, Dynamics, and Online Services' platform and in-scope services.

*Information Security Management*

Management has established an information security policy which defines a common set of security policies and practices that Microsoft Azure, Dynamics, and Online Services teams must follow to help ensure standardized security practices and operation of the IMS. The information security policy includes the security objectives for managing and protecting Microsoft Azure, Dynamics, and Online Services assets and services.

**Performance Evaluation (Clause 9)**

Monitoring, Measurement, Analysis, and Evaluation (Clause 9.1)

Microsoft Azure uses security, privacy, quality, and service delivery KPIs as part of its IMS to help measure performance and effectiveness across its management systems. Annual, independent entity managed assessments are conducted over the design and operating effectiveness of the control environment, which allow monitoring, measurement, and effectiveness of the operating controls. Monitoring is embedded in each service area supporting the SMS.

Senior leadership reviews and amends the KPIs and major milestones as part of the planning process on a semi-annual basis. KPIs are reviewed by management and action items are created and tracked via appropriate security metrics through S360 portal.

Additionally, Microsoft Azure, Dynamics and Online Services monitors the availability of services according to the metrics outlined in SLAs, which are also available to customers via the Azure, Dynamics, and Online Services management portal. Microsoft utilizes several different performance metrics and tools to monitor and ensure customer satisfaction.

Measurement initiatives are conducted on a regular basis at varied frequencies, depending on the metric being monitored. Achieved metrics were formally communicated and reviewed as a component of the leadership meeting in September 2022. It was further noted that the compliance and review meeting included a review of the various audit and compliance programs, as well as status of the ongoing internal programs.

Internal Audit (Clause 9.2)

Microsoft Azure management is committed to perform continuous independent reviews and assessments of its IMS and control environment to help ensure design and operating effectiveness of the controls is assessed and validated on periodic basis.

The most recent internal audit was performed in March 2023, the internal audit report was dated April 7, 2023, and covered the conformance of the SMS to requirements of the ISO 20000-1 standard. The internal audit report included an overall conclusion, audit objectives, scope, audit criteria (inclusive of frequency and methods), assessment of areas reviewed, as well as detailed audit results to support the audit conclusion. The internal audit report was provided to management in April 2023.

Management Reviews (Clause 9.3)

Management reviews are performed to of the SMS and the services, ensuring continuing suitability, adequacy, and effectiveness of the SMS. As noted previously, the IMF's role is to provide management oversight and guidance on the business operations and effectiveness of the SMS via periodic meetings.

Monthly CAI leadership reviews are conducted to discuss progress, monitor changes, and provide input to continuous improvement of the quality KPIs. The leadership reviews ensure the continuing suitability, adequacy, and effectiveness of the SMS.

The most recent monthly CAI leadership review meeting was held on December 12, 2022. Minutes were taken during the meeting and maintained as a record. The minutes include the agenda items as well as associated action items, and future management review meeting topics to be discussed. The minutes also included any outputs taken from the meetings.

Service Reporting (Clause 9.4)

Microsoft Azure management is committed to proper communication with internal and external stakeholder on the relevant state of the IMS. As such, management has defined the IMS communications plan to help identify the interested parties who require information, what information is required, when the information is required, and how that information will be provided to the interested party.

**Improvement (Clause 10)**

Microsoft Azure management is committed to continual improvement of the effectiveness of the SMS through the MSPP, control objectives, audit results, analysis of monitored events, along with corrective and preventive actions and management reviews.

Microsoft Azure management takes corrective action, as needed, to eliminate the cause of nonconformities within the scope of the SMS to help prevent recurrence of control failures and to help reduce the likelihood / impact of future incidents. Procedures are followed when taking corrective action and actions are recorded in the corresponding exception trackers.

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

Microsoft Azure management is committed to the continual improvement and effectiveness of its overarching IMS through the use of the information security policy, privacy policy, information security and privacy control objectives, audit results, analysis of monitored events, along with corrective and preventive actions and management reviews.

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 SMS. 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 leadership meetings. Additionally, the personnel responsible for the SMS continually assess its effectiveness and how the implementation and execution of the SMS can improve.

# SECTION 3

## RECERTIFICATION 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 SMS in relation to the ISO 20000-1 standard requirements, specifically Clauses 4 through 10, that are applicable to the SMS. Documentation requirements as well as the maintenance, monitoring, and operating effectiveness of the SMS have been classified according to their significance in achieving conformance to the standard. The classifications are defined as follows:

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

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

  - **Major: nonconformity that affects the capability of the management system to achieve the intended results**

    *Note 1 to entry: Nonconformities could be classified as major in the following circumstances: 1) if there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements, or 2) a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity.*

  - **Minor: nonconformity that does not affect the capability of the management system to achieve the intended results**
- **Not Applicable (NA)** – The Clause was not applicable to the review.

## RECERTIFICATION REVIEW TESTING RESULTS – SMS FRAMEWORK

| Clause | Subject Audited | Clause Classification | | | | Remarks |
|---|---|---|---|---|---|---|
| | | C | MN | MJ | NA | |
| **4** | **Context of the Organization** | | | | | |
| 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 service management system | ✓ | | | | |
| 4.4 | Service management system | ✓ | | | | |
| **5** | **Leadership** | | | | | |
| 5.1 | Leadership and commitment | ✓ | | | | |
| 5.2.1 | Establishing the service management policy | ✓ | | | | |
| 5.2.2 | Communicating the service management policy | ✓ | | | | |
| 5.3 | Organizational roles, responsibilities, and authorities | ✓ | | | | |
| **6** | **Planning** | | | | | |
| 6.1 | Actions to address risks and opportunities | ✓ | | | | |
| 6.2.1 | Establish objectives | ✓ | | | | |
| 6.2.2 | Plan to achieve objectives | ✓ | | | | |
| 6.3 | Plan the service management system | ✓ | | | | |
| **7** | **Support** | | | | | |
| 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 documented information | ✓ | | | | |
| 7.5.3 | Documented information - Control of documented information | ✓ | | | | |
| 7.5.4 | Documented information - Service management system documented information | ✓ | | | | |
| 7.6 | Documented information - Knowledge | ✓ | | | | |
| **8** | **Operation** | | | | | |
| 8.1 | Operational planning and control | ✓ | | | | |
| 8.2.1 | Service portfolio - General | ✓ | | | | |
| 8.2.2 | Plan the services | ✓ | | | | |

| Clause | Subject Audited | Clause Classification | | | | Remarks |
|---|---|---|---|---|---|---|
| | | C | MN | MJ | NA | |
| 8.2.3 | Control of parties involved in the service lifecycle | ✓ | | | | |
| 8.2.4 | Service catalogue management | ✓ | | | | |
| 8.2.5 | Asset Management | ✓ | | | | |
| 8.2.6 | Configuration Management | ✓ | | | | |
| 8.3.1 | Relationship and agreement - General | ✓ | | | | |
| 8.3.2 | Business relationship management | ✓ | | | | |
| 8.3.3 | Service level management | ✓ | | | | |
| 8.3.4 | Supplier management | ✓ | | | | |
| 8.4.1 | Supply and Demand - Budgeting and accounting for services | ✓ | | | | |
| 8.4.2 | Demand management | ✓ | | | | |
| 8.4.3 | Capacity management | ✓ | | | | |
| 8.5.1 | Service design, build and transition - Change Management | ✓ | | | | |
| 8.5.2 | Service design and transition | ✓ | | | | |
| 8.5.3 | Release and deployment management | ✓ | | | | |
| 8.6.1 | Resolution and fulfilment - Incident Management | ✓ | | | | |
| 8.6.2 | Resolution and fulfilment - Service request management | ✓ | | | | |
| 8.6.3 | Resolution and fulfilment - Problem management | ✓ | | | | |
| 8.7.1 | Service assurance - Service availability management | ✓ | | | | |
| 8.7.2 | Service assurance - Service continuity management | ✓ | | | | |
| 8.7.3 | Service assurance - Information security management | ✓ | | | | |
| **9** | **Performance Evaluation** | | | | | |
| 9.1 | Performance evaluation - Monitoring, measurement, analysis, and evaluation | ✓ | | | | |
| 9.2.1 | Internal audit - General | ✓ | | | | |
| 9.2.2 | Internal audit - Audit programme(s) | ✓ | | | | |
| 9.3 | Management review - General | ✓ | | | | |
| 9.4 | Management review - Service reporting | ✓ | | | | |
| **10** | **Improvement** | | | | | |
| 10.1 | Improvement - Nonconformity and corrective action | ✓ | | | | |
| 10.2 | Continual improvement | ✓ | | | | |

# SECTION 4

## CERTIFICATION CYCLE PROGRAM

## CERTIFICATION CYCLE PROGRAM

| Year | Type of Review | Process to be Reviewed | Audit Time | Locations to be Visited |
|---|---|---|---|---|
| 2023 | Recertification | SMS and full system scope | 8.0 days remote / 1.5 days off-site | Redmond, WA<br>Sample of Data Centers |
| 2024 | Surveillance | SMS and specific scope testing surrounding operations | 3.5 days on-site / 0.5 day off-site | Redmond, WA<br>Sample of Data Centers |
| 2025 | Surveillance | SMS and specific scope testing surrounding operations | 3.5 days on-site / 0.5 day off-site | Redmond, WA<br>Sample of Data Centers |
| 2026 | Recertification | SMS and full system scope | 6.0 days on-site / 1.0 days off-site | Redmond, WA<br>Sample of Data Centers |

Legend

☐ Future projects

# APPENDIX

## MICROSOFT AZURE SCOPE STATEMENT

# MICROSOFT AZURE SCOPE STATEMENT

### Scope of the SMS

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.

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.

### 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 | ✓ | ✓ |
| | Cognitive Services: Translator | ✓ | ✓ |
| | Cognitive Services: QnAMaker Service | ✓ | ✓ |

| Product Category | Service/Offering Name | Cloud Environment Scope | |
|---|---|---|---|
| | | Azure | Azure Government |
| AI + Machine Learning | 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 | ✓ | - |
| | Open AI Enterprise | ✓ | - |
| | Azure Singularity | ✓ | - |
| 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 (VM) 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 | ✓ | ✓ |
| | Service Connector | ✓ | - |

| Product Category | Service/Offering Name | Cloud Environment Scope | |
|---|---|---|---|
| | | Azure | Azure Government |
| **Compute** | Guest Configuration | ✓ | ✓ |
| | Azure VMware Solution | ✓ | - |
| | Planned Maintenance | ✓ | ✓ |
| | Azure Arc-enabled Servers | ✓ | ✓ |
| | Azure Spring Apps | ✓ | - |
| | 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 Apps | ✓ | - |
| | Azure Container Service | ✓ | ✓ |
| | Azure Kubernetes Fleet Manager | ✓ | ✓ |
| **Databases** | Azure Arc-enabled SQL Server | ✓ | - |
| | 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 | ✓ | - |

| Product Category | Service/Offering Name | Cloud Environment Scope | |
|---|---|---|---|
| | | Azure | Azure Government |
| **Developer Tools** | Azure DevTest Labs | ✓ | ✓ |
| | Azure Lab Services | ✓ | ✓ |
| | Azure Load Testing | ✓ | ✓ |
| | Azure for Education | ✓ | - |
| | Azure App Configuration | ✓ | ✓ |
| | GitHub AE | ✓ | ✓ |
| **Identity** | Azure Information Protection | ✓ | ✓ |
| | Azure Active Directory | ✓ | ✓ |
| | 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 | ✓ | ✓ |
| | Device Update for IoT Hub | ✓ | - |
| | Azure Sphere | ✓ | - |
| | Azure Time Series Insights | ✓ | - |
| | Windows 10 IoT Core Services | ✓ | - |
| | 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 | ✓ | ✓ |

| Product Category | Service/Offering Name | Cloud Environment Scope | |
|---|---|---|---|
| | | Azure | Azure Government |
| Management and Governance | Azure Managed Applications | ✓ | ✓ |
| | Azure Managed Grafana | ✓ | - |
| | Azure Migrate | ✓ | ✓ |
| | Azure Monitor | ✓ | ✓ |
| | Azure Policy | ✓ | ✓ |
| | Azure Resource Graph | ✓ | ✓ |
| | Cloud Shell | ✓ | ✓ |
| | Microsoft Azure Portal | ✓ | ✓ |
| | Azure Blueprints | ✓ | - |
| | 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 | ✓ | ✓ |

| Product Category | Service/Offering Name | Cloud Environment Scope | |
|---|---|---|---|
| | | Azure | Azure Government |
| **Networking** | Azure Web Application Firewall | ✓ | ✓ |
| | Content Delivery Network | ✓ | ✓ |
| | Network Watcher | ✓ | ✓ |
| | Traffic Manager | ✓ | ✓ |
| | Virtual WAN | ✓ | ✓ |
| | Azure Public IP | ✓ | ✓ |
| | Virtual Network NAT | ✓ | ✓ |
| | Azure Network Function Manager | ✓ | - |
| | Azure Route Server | ✓ | ✓ |
| | Azure Virtual Network Manager | ✓ | - |
| **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 Azure 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 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 | ✓ | ✓ |

| Product Category | Service/Offering Name | Cloud Environment Scope | |
|---|---|---|---|
| | | Azure | Azure Government |
| Web | Azure Fluid Relay | ✓ | - |
| | Azure Maps | ✓ | ✓ |
| | Azure SignalR Service | ✓ | ✓ |
| | Azure Web PubSub | ✓ | ✓ |
| 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 | | ✓ | ✓ |
| Azure Public MEC | | ✓ | - |
| Power Virtual Agents | | ✓ | ✓ |
| Microsoft Threat Experts | | ✓ | - |
| Nomination Portal | | ✓ | ✓ |
| Microsoft 365 Defender | | ✓ | ✓ |
| Microsoft Defender for Endpoint | | ✓ | ✓ |
| Microsoft Defender for Identity | | ✓ | ✓ |
| Microsoft Bing for Commerce | | ✓ | - |
| Universal Print | | ✓ | - |
| Update Compliance | | ✓ | - |
| Azure Managed Experience | | ✓ | - |
| Windows Autopatch | | ✓ | - |
| **Microsoft Dynamics 365** | | | |
| Dynamics 365 Customer Service | | ✓ | ✓ |
| Dynamics 365 Customer Insights Engagement Insights | | ✓ | - |
| Dynamic 365 Customer Voice | | ✓ | ✓ |

| Product Category | Service/Offering Name | Cloud Environment Scope | |
|---|---|---|---|
| | | Azure | Azure Government |
| Dynamics 365 Field Service | | ✓ | ✓ |
| Dynamics 365 Sales | | ✓ | ✓ |
| Dynamics 365 Sales Professional | | ✓ | - |
| Dynamics 365 Sales Insights | | ✓ | - |
| Dynamics 365 AI Customer Insights | | ✓ | ✓ |
| Dynamics 365 Business Central | | ✓ | - |
| Dynamics 365 Finance | | ✓ | ✓ |
| Dynamics 365 Fraud Protection | | ✓ | - |
| Dynamics 365 Marketing | | ✓ | - |
| Power Pages | | ✓ | ✓ |
| 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 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 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 SMS | |
|---|---|
| Redmond, Washington | One Microsoft Way<br>Redmond, Washington 98052<br>United States |

| Microsoft Azure Domestic Datacenters | |
|---|---|
| West US | Santa Clara, CA (BY1/3/4/5/21/22/24/30)<br>San Jose, CA (SJC20/21/22/31) |
| West US 2 | Quincy, WA (CO1/2/6, MWH01/02/03/04/05/06/20/21) |
| 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, SAT09/10/11/12/20) |
| East US | Bristow, VA (BLU)<br>Reston, VA (BL4)<br>Sterling, VA (BL20)<br>Ashburn, VA (BL2/3/5/6/7/21/22/23/24/30/31)<br>Manassas, VA (MNZ20/22/26)<br>Dulles, VA (IAD01/20)<br>Lawrenceville, GA (LVL03/08) |
| 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 (PHX20/21/22/23) |
| US GOV Texas | San Antonio, TX (SN5/SAT21) |
| US GOV Virginia | Boydton, VA (BN1/11/12) |
| US GOV Wyoming | Cheyenne, WY (CYS01) |

| Microsoft Azure International Datacenters | |
|---|---|
| Canada East | Quebec, Canada (YQB20) |
| Canada Central | Toronto, Canada (YTO20/21/22/23/24) |
| Brazil South | Campinas, Brazil (CPQ01/02/20/21/22/23/24/25)<br>Sao Paulo, Brazil (GRU) |
| Brazil Southeast | Rio de Janeiro, Brazil (RIO01/20) |
| West Europe | Amsterdam, Netherlands (AM3, AMS04/05/06/07/08/09/11/12/20/21/22/23/24/25) |
| North Europe | Dublin, Ireland (DB3/4/5, DUB06/07/08/09/10/12/13/20/21/24/25/26/31) |
| UK South | London, United Kingdom (LON21/22/23/24/25/26/27/28) |
| UK West | Cardiff, United Kingdom (CWL20) |
| France Central | Paris, France (PAR20/21/22/23/24/25/27) |
| France South | Marseille, France (MRS20/21) |
| Germany North | Berlin, Germany (BER20/21) |
| Germany West Central | Frankfurt, Germany (FRA21/22/23) |
| Germany Central | Frankfurt, Germany (FRA20) |
| Sweden Central | Gavleborg, Sweden (GVX01/02/11/21) |
| Sweden South | Malmo, Sweden (MMA01) |
| Switzerland West | Geneva, Switzerland (GVA20) |
| Switzerland North | Zurich, Switzerland (ZRH20/21/22) |
| East Asia | Hong Kong (HK2, HKG20/21/22/23) |
| Southeast Asia | Singapore (SG2/3, SIN06/20/21/22) |
| 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 (OSA01/02/20/21/22/23) |
| 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)<br>Sydney, Australia (SYD21/22/23/24/25/26/27/28) |
| Australia Southeast | Melbourne, Australia (MEL01/20/21/23/24) |
| Australia Central | Canberra, Australia (CBR20/22) |

| Microsoft Azure International Datacenters | |
|---|---|
| Australia Central 2 | Canberra, Australia (CBR21/23) |
| South Africa North | Johannesburg, South Africa (JNB20/21/22/23) |
| South Africa West | Cape Town, South Africa (CPT20/21) |
| Norway East | Oslo, Norway (OSL20/21/22/23/24) |
| Norway West | Stavanger, Norway (SVG20) |
| Qatar Central | Doha, Qatar (DOH20/21/22/23) |
| Israel Central | Tel Aviv-Yafo, Israel (TLV20) |

| Microsoft Online Services Datacenters | |
|---|---|
| Southeast Asia 2 | Cyberjaya, Malaysia (KUL01/JHB20) |
| Korea South 2 | Busan, South Korea (PUS01) |
| Brazil Northeast | Fortaleza, Brazil (FOR01) |
| Chile Central | Santiago, Chile (SCL01/20/21) |
| Austria East | Vienna, Austria (VIE/VIE20) |
| North Europe 2 | Vantaa, Finland (HEL01) |

| Edge Sites | |
|---|---|
| Ashburn, VA (ASH) | Manila, Philippines (MNL30) |
| Athens, Greece (ATH01) | Memphis, TN (MEM30) |
| Atlanta, GA (ATA) | Minneapolis, MN (MSP30) |
| Auckland, New Zealand (AKL30) | Miami, FL (MIA) |
| Bangkok, Thailand (BKK30) | Milan, Italy (MIL30) |
| Barcelona, Spain (BCN30) | Montreal, Canada (YMQ01) |
| Barueri, Brazil (GRU30) | Moscow Russia (MOW30) |
| Berlin, Germany (BER30) | Mumbai, India (BOM02) |
| Bogota, Columbia (BOG30) | Munich, Germany (MUC30) |
| Boston, MA (BOS31) | Nairobi, Kenya (NBO30) |
| Brisbane, Australia (BNE01) | Nashville, TN (BNA30) |
| Brussels, Belgium (BRU30) | New Delhi, India (DEL01) |
| Bucharest, Romania (BUH01) | New York City, NY (NYC) |
| Budapest, Hungary (BUD01) | Newark, NJ (EWR30) |
| Buenos Aires, Argentina (BUE30) | Osaka, Japan (OSA30/31) |
| Busan, South Korea (PUS03) | Oslo, Norway (OSL30) |
| Cairo, Egypt (CAI30) | Palo Alto, CA (PAO) |
| Cape Town, South Africa (CPT02) | Paris, France (PAR02/PRA) |
| Chennai, India (MAA02) | Perth, Australia (PER01/30) |
| Chicago, IL (CHG/CHI30) | Philadelphia, PA (PHL30) |

| Edge Sites | |
|---|---|
| Cincinnati, OH (CVG30) | Phoenix, AZ (PHX31) |
| Copenhagen, Denmark (CPH30) | Portland, OR (PDX31) |
| Dallas, TX (DAL, DFW30) | Prague, Czech Republic (PRG01) |
| Denver, CO (DNA) | Pune, India (PNQ30) |
| Doha, Qatar (DOH30/31) | Queretaro, Mexico (MEX30/31) |
| Dubai, United Arab Emirates (DXB30) | Rabat, Morocco (RBA30) |
| Dusseldorf, Germany (DUS30) | Rio De Janeiro, Brazil (RIO02/03) |
| Frankfurt, Germany (FRA31) | Rome, Italy (ROM30) |
| Geneva, Switzerland (GVA30) | Salt Lake City, UT (SLC31) |
| Helsinki, Finland (HEL02/03) | Sao Paulo, Brazil (SAO03/31) |
| Ho Chi Minh, Vietnam (SGN30) | San Diego, California (SAN30) |
| Hong Kong (HKB/HKG30) | San Jose, CA (SJC) |
| Honolulu, HI (HNL01) | Santiago, Chile (SCL30) |
| Houston, TX (HOU01) | Seattle, WA (STB/WST) |
| Hyderabad, India (HYD30) | Seoul, South Korea (SLA) |
| Istanbul, Turkey (IST30) | Singapore (SGE, SG1, SIN30) |
| Jacksonville, FL (JAX30) | Sofia, Bulgaria (SOF01) |
| Jakarta, Indonesia (JKT30) | Stockholm, Sweden (STO) |
| Johannesburg, South Africa (JNB02) | Taipei, Taiwan (TPE30/31) |
| Kiev, Ukraine (IEV30) | Tampa, FL (TPA30) |
| Kuala Lumpur, Malaysia (KUL02/30) | Tel Aviv, Israel (TLV30) |
| Las Vegas, NV (LAS01/30) | Teterboro, NJ (TEB31) |
| Lisbon, Portugal (LIS01) | Tokyo, Japan (TYA/TYB) |
| Los Angeles, CA (LAX) | Toronto, Canada (YTO01/30) |
| Lagos, Nigeria (LOS30) | Vancouver, Canada (YVR30) |
| London, United Kingdom (LON04, LTS) | Warsaw, Poland (WAW01) |
| Luanda, Angola (LAD30) | Zagreb, Croatia (ZAG30) |
| Madrid, Spain (MAD30) | Zurich, Switzerland (ZRH) |
| Manchester, United Kingdom (MAN30) | |

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