NOTICE: You and your company have obtained access to this report on the description of the system of Microsoft Corporation – Microsoft 365 Online Services (Delta) ("this SOC 1 Report") by accepting the terms of the Access Agreement that was attached to this SOC 1 Report and acknowledging that your company is a prospective customer of Microsoft Corporation – Microsoft 365 Online Services (Delta) ("Microsoft 365"). The terms of the Access Agreement include, among other things, an agreement by you and your company not to further disclose, distribute, quote, or reference this SOC 1 Report and an agreement to release and indemnify Deloitte & Touche LLP ("Deloitte & Touche"), its subsidiaries and its subcontractors, and their respective personnel. By reading this SOC 1 Report, you reconfirm your agreement to the terms of such Access Agreement. If you are not a prospective customer of Microsoft 365 then you are not authorized to possess, read, or have access to this SOC 1 Report and should immediately return this SOC 1 Report to Microsoft 365.

This SOC 1 Report is intended only to be used by Microsoft 365's existing clients as of May 15, 2025, and their external auditors (i.e., "user entities" as of May 15, 2025, and the "user auditors" as of May 15, 2025, respectively, as stated in the independent service auditor's report contained in this SOC 1 Report and defined in the American Institute of Certified Public Accountants ("AICPA") Attestation Standards and International Auditing and Assurance Standards Board's International Standard on Assurance Engagements (ISAE) 3402 (ISAE 3402) ("Permitted Users"). Deloitte & Touche, the entity that issued the independent service auditors' report contained in this SOC 1 Report, its subsidiaries and subcontractors, and their respective personnel shall have no liability, duties, responsibilities or other obligations to any entity who may obtain this SOC 1 Report who is not a Permitted User, including, without limitation, any entity who obtains this SOC 1 Report in contemplation of contracting for services with Microsoft 365.

Deloitte & Touche, its subsidiaries and subcontractors, and their respective personnel have no responsibility for the description of the system of Microsoft 365, including the control objectives and the controls. Nor do Deloitte & Touche, its subsidiaries and subcontractors, and their respective personnel have any obligation to advise or consult with any entity regarding their access to this SOC 1 Report. Any use of this SOC 1 Report by a party other than a Permitted User ("Other Third Party") is at the sole and exclusive risk of such Other Third Party and such Other Third Party cannot and shall not rely on this SOC 1 Report. This SOC 1 Report is not to be further disclosed, distributed, quoted, or referenced to any third party or included or incorporated by reference in any other document, including any securities filings.

Microsoft Corporation—Microsoft 365 Online Services (Delta)

System and Organization Controls (SOC) 1 Report

May 15, 2025

Deloitte.

This report is intended solely for the information and use of management of Microsoft, user entities of Microsoft's M365 Online Services (Delta) system as of May 15, 2025, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Table of Contents

Executive Summary

Microsoft Corporation—Microsoft 365 Online Services (Delta)	
Scope	Cloud Input Intelligence (CII)
As of	May 15, 2025
Location(s)	Redmond, Washington (WA)
Subservice Providers	Yes – • Microsoft Azure (“Azure”) including Microsoft Datacenters • Microsoft 365 Central Services (“M365 Central”)
Opinion Result	Unqualified
Controls with Testing Exceptions	0
Complementary User-Entity Controls	Yes – See **Page 29**
Complementary Subservice Organization Controls	Yes – See **Page 30**

Section 1:
Independent Service Auditor’s Report

Deloitte & Touche LLP
1015 Second Avenue, Suite 500
Seattle, WA 98104
Tel: +1 206 716 7000
Fax: +1 206 965 7000
www.deloitte.com

Section 1:
Independent Service Auditor's Report

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Scope

We have examined the description of the Microsoft 365 Online Services (Delta)[1] system of Management of Microsoft Corporation (the "Service Organization" or "Microsoft") for processing user entities' transactions as of May 15, 2025, included in **Section 3**, "Management of Microsoft's Description of Its Microsoft 365 Online Services (Delta) System" (the "Description") and the suitability of the design and implementation of controls included in the Description to achieve the related control objectives stated in the Description, based on the criteria identified in management of Microsoft's assertion. The controls and control objectives included in the Description are those that management of Microsoft believes are likely to be relevant to user entities' internal control over financial reporting, and the Description does not include those aspects of the M365 Online Services (Delta) system that are not likely to be relevant to user entities' internal control over financial reporting.

The information in **Section 4**, "Supplemental Information Provided by Management of Microsoft" is presented by management of Microsoft to provide additional information and is not a part of management of Microsoft's Description of its M365 Online Services (Delta) system made available to user entities as of May 15, 2025. Information in **Section 4** has not been subjected to the procedures applied in the examination of the Description of the M365 Online Services (Delta) system and of the suitability of the design and implementation of controls to achieve the related control objectives stated in the Description of the M365 Online Services (Delta) system and, accordingly, we express no opinion on it.

Microsoft uses Microsoft Azure, including the Microsoft Datacenters service, for its hosting of physical and virtual servers, network management, data protection and storage services. Additionally, Microsoft uses M365 Central Services shared services and supporting technology to support the IT environment including logical access, server baselines, incident management, restoration of customer content, and vulnerability scanning ("subservice organizations"). The Description in **Section 3** includes only the controls and related control objectives of Microsoft and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified by Microsoft can be achieved only if complementary subservice organization controls assumed in the design of Microsoft's controls are suitably designed and operating effectively, along with the related controls at Microsoft. Our examination did not extend to controls of the subservice organizations or their functions, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

---

1 In-scope services are defined in Section 3 of this SOC Report. These in-scope services are referred to throughout this report as "M365 Online Services (Delta)." Items relating to the overall Microsoft 365 service will be referred to as "M365."

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of Microsoft's controls are suitably designed and operating effectively, along with related controls at Microsoft. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section 2, "Management of Microsoft's Assertion," management of Microsoft has provided an assertion about the fairness of the presentation of the Description and the suitability of the design and implementation of the controls to achieve the related control objectives stated in the Description. Management of Microsoft is responsible for preparing the Description and its assertion, including the completeness, accuracy, and method of presentation of the Description and the assertion, providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the Description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and implementation of the controls to achieve the related control objectives stated in the Description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3402, Assurance Reports on Controls at a Service Organization, issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the Description is fairly presented, and the controls were suitably designed to achieve the related control objectives stated in the Description as of May 15, 2025. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a Description of a service organization's system and the suitability of the design and implementation of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and implementation of the controls to achieve the related control objectives stated in the Description, based on the criteria in management's assertion.
- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed to achieve the related control objectives stated in the Description.
- Evaluating the overall presentation of the Description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service organization in its assertion.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants. We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and the International Standards on Quality Management issued by the IAASB and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and therefore may not include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design and implementation of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the Description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects, based on the criteria described in management of Microsoft's assertion:

a. The Description fairly presents the M365 Online Services (Delta) system that was designed and implemented as of May 15, 2025.

b. The controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively as of May 15, 2025, and the subservice organizations and user entities applied the complementary controls assumed in the design of Microsoft's controls as of May 15, 2025.

Restricted Use

This report is intended solely for the information and use of management of Microsoft, user entities of Microsoft's M365 Online Services (Delta) system as of May 15, 2025, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Deloitte & Touche LLP

June 30, 2025

Section 2:
Management of Microsoft's Assertion

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Section 2:
Management of Microsoft's Assertion

Management of Microsoft's Assertion

As of May 15, 2025

We have prepared the description of the Microsoft 365 Online Services (Delta)[2] system of Management of Microsoft Corporation (the "Service Organization" or "Microsoft") for processing user entities' transactions as of May 15, 2025, included in **Section 3**, "Management of Microsoft's Description of Its Microsoft 365 Online Services (Delta) System" (the "Description"), for user entities of the system as of May 15, 2025, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when obtaining an understanding of user entities' information and communication systems relevant to financial reporting.

Microsoft uses Microsoft Azure, including the Microsoft Datacenters service, for its hosting of physical and virtual servers, network management, data protection and storage services. Additionally, Microsoft uses M365 Central Services shared services and supporting technology to support the IT environment including logical access, server baselines, incident management, restoration of customer content, and vulnerability scanning ("subservice organizations"). The Description in **Section 3** includes only the controls and related control objectives of Microsoft and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified by Microsoft can be achieved only if complementary subservice organization controls assumed in the design of Microsoft's controls are suitably designed and operating effectively, along with the related controls at Microsoft. The Description does not extend to controls of the subservice organizations.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of Microsoft's controls are suitably designed and operating effectively, along with related controls at Microsoft. The Description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

1. The Description fairly presents the M365 Online Services (Delta) system made available to user entities of the system as of May 15, 2025, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description:
    a. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable:
        i. The types of services provided including, as appropriate, the classes of transactions processed.
        ii. The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated,

[2] In-scope services are defined in Section 3 of this SOC Report. These in-scope services are referred to throughout this report as "M365 Online Services (Delta)." Items relating to the overall Microsoft 365 service will be referred to as "M365."

authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

iii. The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

iv. How the system captures and addresses significant events and conditions other than transactions.

v. The process used to prepare reports and other information provided for user entities.

vi. Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

vii. The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the service organization's controls.

viii. Other aspects of our control environment, risk assessment process, information, and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

b. Does not omit or distort information relevant to the service organization's system, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the M365 Online Services (Delta) system that each individual user entity of the system and its user auditor may consider important in its own particular environment.

2. The controls related to the control objectives stated in the Description were suitably designed and implemented as of May 15, 2025, to achieve those control objectives if the subservice organization and user entities applied the complementary controls assumed in the design of Microsoft's controls as of May 15, 2025. The criteria we used in making this assertion were that:

   a. The risks that threaten the achievement of the control objectives stated in the Description have been identified by management of Microsoft.

   b. The controls identified in the Description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved.

Section 3:
Management of Microsoft's Description of Its Microsoft 365 Online Services (Delta) System

Section 3:
Management of Microsoft's Description of Its Microsoft 365 Online Services (Delta) System

Overview of Operations

Business Description

Microsoft Corporation's (Microsoft) Microsoft 365 Online Services' (Delta) systems[3] are components of Microsoft 365 ("M365"), a subscription-based business software service hosted by Microsoft and sold directly, or with partners, to various customers worldwide. M365 services are designed to provide performance, scalability, security, management capabilities, and service levels required for mission-critical applications and systems used by business organizations. The scope of this SOC 1 Type 1 attestation is limited to controls covering the M365 Online Services' (Delta) systems; however, due to how these systems are hosted within M365's environment, we deemed it necessary to also include a description of those aspects of M365's environment that directly support the M365 Online Services (Delta).

Cloud Input Intelligence (CII) is a service that processes ink strokes of different texts and shapes and returns a breakdown of what the ink represents on a digital flowchart.

M365 Online Services (Delta) is physically hosted in Microsoft-managed datacenters. Microsoft Datacenters is managed and run by Microsoft Azure, and both Microsoft Datacenters and Microsoft Azure are treated as one subservice organization (Azure) but will be referred to separately in this report to clarify which part of the Azure organization is responsible for the different services. Both services are not within the scope of this report. The M365 Online Services (Delta) rely on different functions of the M365 Central Services, including but not limited to data encryption, restorations, security and incident management, and vulnerability scanning.

Microsoft Azure, including Microsoft Datacenters, and M365 Central Services are treated as subservice organizations and are not within the scope of this report.

Applicability of The Report

This report has been prepared to provide information on M365 Online Services' (Delta) internal controls that may be relevant to the requirements of its customers and affect the processing of user entities' transactions. The detail herein is intended to meet the common requirements of a broad range of users and may not, therefore, include every aspect of the system that each customer may consider important. Furthermore, detail is limited to the controls in operation over the system as defined in the M365 scope boundary described below. The authorized users of the system supporting the internal controls are limited to M365 personnel.

This report covers the following M365 online service:

- Cloud Input Intelligence (CII)

Infrastructure

M365 Online Services (Delta) is hosted by Microsoft Azure, including Microsoft Datacenters. This includes: (1) Microsoft Datacenters Infrastructure as a Service (IaaS) and (2) Azure's IaaS and Platform as a Service (PaaS).

---

[3] In-scope services are defined in Section 3 of this SOC Report. These in-scope services are referred to throughout this report as "M365 Online Services (Delta)." Items relating to the overall Microsoft 365 service will be referred to as "M365."

For Microsoft Datacenters hosting, the physical servers are owned by M365, the Operating System (OS) and software are managed by M365, and network layer protections are implemented by Microsoft Datacenters. M365 manages the configuration of the network layer/protection in coordination with Microsoft Datacenters.

For Azure's IaaS hosting, M365 is responsible for the OS and database management. For Azure PaaS hosting, M365 is responsible for limited configurations of the OS, while Azure is responsible for database and storage setup and maintenance and overall OS setup and protections. Network layer protections are implemented by Azure for both IaaS and PaaS and are managed in coordination with Azure.

In both cases, Microsoft Datacenters is responsible for physical and environmental security. In addition, Azure's PaaS provides customer authentication and rights management services through Microsoft Entra ID (formerly Azure Active Directory (AAD)). The controls managed by Microsoft Azure, including Microsoft Datacenters, are audited separately and therefore are not within the scope of this report.

Software

This report applies to the M365 Online Services (Delta) including Cloud Input Intelligence (CII), as described previously. This M365 Online Services (Delta) service is supported by the following M365 Central Services software that are not directly covered in this report:

- Identity Manager (IDM) – An access management service providing an integrated and broad solution for managing M365 user identities and associated credentials for all M365 applications.
- Microsoft 365 (M365) Remote Access – A set of servers providing remote access to M365 service production environments via authorized two-factor authentication and encryption.

In addition to the product software, the following utilities are used by the service teams to execute controls relevant to the M365 system but are not directly covered in this report:

- Employee Cloud Screening (ECS) – A Human Resources (HR) SAP interface used by Microsoft Human Resources that hosts employee background check information that synchronizes with IDM databases to limit user access to eligibilities based on background check status.
- Substrate, Office Substrate Pulse (OSP) – A platform and system tools for centrally managing and hosting applications and services that are used internally by M365 and by customers.
- Qualys – Scanning systems used to identify and resolve security vulnerabilities within the M365 environment.
- IDWeb, OneIdentity, and Torus – M365 user management tools used to grant temporary user access time-bound permissions and access to sensitive systems, including access to customer content.
- Remote Desktop Services – The accepted method for Microsoft personnel to gain logical access to the M365 environment remotely using Remote Desktop Gateways (RDGs).
- Griffin, Office Supporting Infrastructure (OSI), M365SuiteUX Environments and Release Dashboard, PilotFish, and Azure DevOps – Change management tools used by service and support teams to track and deploy code changes to production environments.
- Aria, Geneva, Incident Manager (IcM), and Jarvis – Dashboards and alerting systems that monitor the capacity and availability of the servers and services based on pre-determined capacity and availability thresholds. In the event of a breach of a capacity or availability threshold, automated alerts are generated and communicated to the service team's respective on-call engineer for tracking and remediation. Additionally, they provide a visual representation of major/minor system releases across various stages including preproduction, testing, and production.
- M365 UAR Tool – A user access review tool designed to enable service teams to identify resources and perform a review of privileged access.

People

M365 personnel are organized into service teams that develop and maintain the application and support teams that provide supporting services for system operations.

Each service and support team for M365 has defined responsibilities and accountabilities to manage the security, availability, processing integrity, and confidentiality of the applications. The teams include the following groups:

- Access Security – Personnel that maintain Active Directory (AD) services, authentication rules, and user access. Operates the IDM tool to provide access control automation for all teams.
- Change Management – Development, testing, and project management teams tasked with developing and maintaining the M365 applications and supporting services.
- Data Redundancy – Personnel for configuring and monitoring the replication of specified internal and customer content for data availability, business continuity, and resiliency.
- Security and Availability Monitoring – Personnel that monitor the incidents that affect the security and availability of M365 applications and supporting services.

In addition to service teams, centralized support teams provide specialized functions for the services, including the following:

- Enterprise Business Continuity Management (EBCM) – A single resource to assist M365 teams in analyzing continuity and disaster recovery requirements, documenting procedures, and conducting testing of established procedures.
- M365 Security – Manages cross-platform security functions, such as security incident response, security monitoring, and vulnerability scanning. This team also develops and enforces the Secure Development Lifecycle process for M365 applications and support services.
- Governance, Risk, and Compliance (GRC) – Identifies, documents, and advises teams in implementing controls to maintain M365's availability and security commitments to its customers.
- Digital Security and Resilience (DSR) – Provides the access control and authentication mechanism for some service teams via IDWeb.
- Azure – Provides customer authentication infrastructure including Microsoft Online Directory Services, Microsoft Organization ID, and Microsoft Entra ID (formerly AAD).
- Microsoft 365 (M365) Remote Access – Provides internal users remote access control and authentication to the M365 environment.

Procedures

M365 adheres to Microsoft Corporation's Security Policy. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses:

- Human resources security
- Asset management
- Asset control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- Systems acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Business continuity management
- Compliance

M365 uses National Institute of Standards and Technology (NIST) standard 800-53 for baseline control procedures, which are documented in the M365 control framework. Control measures above and beyond NIST 800-53 are included to address the full range of Microsoft contractual and regulatory commitments. The framework covers the following areas:

- Access Control
- Accountability, Audit, and Risk
- Authority and Purpose
- Awareness and Training
- Configuration Management
- Contingency Planning
- Data Minimization and Retention
- Data Portability
- Data Quality and Integrity
- Geographic Boundaries
- Identification and Authentication
- Incident Response
- Individual Participation and Redress
- Maintenance
- Media Protection
- Personnel Security
- Physical Access
- Program Management
- Risk Assessment
- Security
- Security Assessment
- Security Planning
- System Access
- System and Communication Security
- System and Information Integrity
- System and Services Acquisition
- Use Limitation

In addition to the above procedures, manual and automated control activities are described in the section "Description of Control Activities" below.

Data

M365 customer content is maintained in Azure and SQL server databases. Each service and support team is responsible for managing the security, availability, processing integrity, and confidentiality of the data in Azure or on the database servers. The table below details the data classifications for this report and the M365 environment.

Data Classification	Definition
Access Control Data	Data used to manage access to administrative roles or sensitive functions.
Customer Content	This is the data, information, and code that admins and users provide to, transfer in, store in, or process in the Microsoft online service or product.
End User Identifiable Information (EUII)	Data that directly identifies or could be used to identify the authenticated user of a Microsoft service.
Organization Identifiable Information (OII)	Data that can be used to identify a particular tenant/Azure subscription/ deployment/organization (generally configuration or usage data): • Not linkable to an individual user • Does not contain customer content
System Metadata	Data generated in the course of running the service, not linkable to a user or tenant. Does not contain Access Control Data, Customer Content, EUII, OII, or Account Data.
Account Data	Contact and billing/purchase/payment/license information for the enterprise, including the admin and any subdelegated admins.

Control Environment

Integrity and Ethical Values

Corporate governance at Microsoft starts with a Board of Directors that establishes, maintains, and monitors standards and policies for ethics, business practices, and compliance that span the company. Corporate governance at Microsoft serves several purposes:

- To establish and preserve management accountability to Microsoft's owners by distributing rights and responsibilities among Microsoft Board members, Managers, and Shareholders.
- To provide a structure through which management and the Board set and attain objectives and monitor performance.
- To strengthen and safeguard a culture of business integrity and responsible business practices.
- To encourage the efficient use of resources and to require accountability for the stewardship of these resources.

Further information about Microsoft's general corporate governance is available on the Microsoft website, www.microsoft.com.

Microsoft's Standards of Business Conduct

Microsoft's Standards of Business Conduct ("SBC") reflect a commitment to ethical business practices and regulatory compliance. They summarize the principles and policies that guide Microsoft's business activities and provide information about Microsoft's Business Conduct and Compliance Program. The SBC was developed in full

consideration of the Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley") and NASDAQ listing requirements related to codes of conduct.

Further information about Microsoft's SBC is available on the Microsoft website, www.microsoft.com.

Training and Accountability

M365 leverages the Microsoft Corporate SBC to provide employees with education and resources to make informed business decisions and to act on their decisions with integrity. SBC training and awareness is provided to Microsoft employees (including M365), contractors, and third parties on an ongoing basis to educate them on applicable policies, standards, and information security practices. Full-time employees must also take a mandatory SBC training course upon being hired, and again on an annual basis thereafter. In addition, employees are required to participate in mandatory security and compliance training periodically to design, build, and operate secure cloud services.

M365 staff and contingent staff are accountable for understanding and adhering to the guidance contained in the Microsoft Security Policy and applicable supporting standards. Individuals not employed by M365, but allowed to access, manage, or process information assets of M365, are also accountable for understanding and adhering to the guidance contained in the Microsoft Security Policy and associated standards.

Commitment to Competence

Microsoft hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities and tasks involved in the job, background characteristics needed to perform the job, and personal characteristics required. Once the requirements are determined, managers create a job description, which is a profile of the job, and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and to make appropriate hiring decisions.

Microsoft employees create individual accountabilities that align with those of their managers, organizations, and Microsoft, and are supported by customer-centric actions and measures so that everyone is working toward the same overarching vision. Accountabilities are established when an employee is hired and then updated throughout the year according to business circumstances.

Managers work with their employees to analyze progress against accountabilities and to adjust accountabilities, if needed, several times throughout the year. Managers evaluate individual contributions to teams, the business, or customer impact, taking into consideration contributions aimed at creating a high performing team and the demonstration of competencies relevant to the role.

Compliance and Ethics — Board of Directors and Senior Leadership

Compliance and Ethics designs and provides reports to the Board of Directors on compliance matters. Compliance and Ethics also organizes annual meetings with the Senior Leadership team for its compliance review.

Internal Audit Department

Microsoft has an Internal Audit (IA) function that reports directly to the Audit Committee (AC) of the Board of Directors, which is constituted solely of independent directors. IA has a formal charter that is reviewed by the AC and management. The responsibilities of IA include performing audits and reporting issues and recommendations to management and the AC.

Audit Committee

The AC charter and responsibilities are on Microsoft's website, www.microsoft.com. The AC meets privately on a quarterly basis with Microsoft's external auditors and IA. The topics for the quarterly AC meetings are found in the AC Responsibilities Calendar set out in the charter. In addition, the AC influences the company through the IA

function. The AC reviews the scope of IA and advises on the process of identifying and resolving issues. Lastly, the AC monitors itself by completing an annual self-evaluation.

Risk Assessment

Practices for Identification of Risk

IA, the Financial Compliance group, and the Finance Risk group perform formal risk identification processes each year. These assessments cover risks over financial reporting, fraud, and compliance with laws.

Internal Audit — Fraud Risks

IA and the Financial Integrity Unit (FIU) look for fraud risk. The FIU performs procedures for the detection, investigation, and prevention of financial fraud affecting Microsoft worldwide. Fraud and abuse that is uncovered is reported to the Disclosure Committee. The FIU provides both a reactive and proactive response to allegations of fraud and abuse. The FIU uses a case management system that is also used by the Director of Compliance to track cases and related metrics. The FIU interacts with Microsoft management, Corporate, External, and Legal Affairs (CELA), HR, Finance, Procurement, and others to determine specific fraud risks and responses.

Periodic Risk Assessment

IA and other groups within the company perform periodic risk assessments. The assessments are reviewed by senior management.

IA specialization area leaders determine high-priority risks across the company, including risks related to financial reporting, operational business processes, and systems controls. Control failures are also analyzed to determine whether they give rise to additional risks.

Annual Risk Assessment

The annual risk assessment process is established to monitor, manage, and mitigate specific business risks related to security for customers and partners. Led by the Risk Management office, Microsoft follows an established approach to risk management and conducts an annual global risk assessment beginning in the first quarter of each fiscal year. The purpose of the annual risk assessment is to identify and prioritize each division's specific strategic and operational risks based on impact, likelihood, and management control. Additionally, accountability is established for each risk and mitigation decisions are made at the Corporate Vice President level with transparency across the leadership team.

Compliance and Ethics/IA/Risk Management — Risk Responsibility

The responsibility for risk is distributed throughout the organization based on each individual group's services. Compliance and Ethics, IA, and the Risk Management Group work together to represent enterprise risk management. Through quarterly and year-end reviews, the Chief Financial Officer (CFO) and Corporate Controller (and respective groups) review the disclosures and issues that may have arisen.

Information and Communication

Internal Communication

Responsibilities concerning internal control are communicated broadly, which include Monthly Controller calls, All Hands Meetings run by the CFO, and update conference calls held by the Financial Compliance Group with the Sarbanes-Oxley extended project team. Responsibilities for compliance with policies are set out in the SBC, for which a mandatory training has been established for all employees. Additionally, compliance managers meet with control owners to make sure they understand the controls for which they are accountable and update the controls based on changes in the business environment.

Office of the CFO — Communications External to the Company

CFO communications outside the company occur throughout the year and, where applicable, these external communications include discussions of the company's attitude toward sound internal controls. The Office of the CFO is responsible for several communications outside of Microsoft including quarterly earnings releases, financial analyst meetings, customer visits, outside conferences, and external publications.

Monitoring

Compliance and Ethics — Business Conduct Hotline

There is a confidential and anonymous Business Conduct Hotline available for employees to report issues. The hotline is accessible 24 hours per day and 7 days per week through email, phone, fax, the Microsoft Integrity Web site, and mail. The individual may also send a letter or fax reporting the concern to Microsoft's Director of Compliance. Employees are instructed that it is their duty to promptly report concerns of suspected or known violations of the Code of Professional Conduct, the SBC, or other Microsoft policies or guidelines. The procedures to be followed for such a report are outlined in the SBC and the Whistle Blowing Reporting Procedure and Guidelines in the Employee Handbook. Employees are also encouraged to communicate the issue to their Manager, Senior Leadership, CELA contact, HR contact, or the Compliance Office.

Internal Audit

Microsoft's IA department provides support to management across the company by independently and objectively analyzing whether the objectives of management are adequately performed, as well as facilitating process improvements and the adoption of business practices, policies, and controls governing worldwide operations.

Monitoring of Subservice Organizations

M365 Online Services (Delta) uses the following subservice organizations:

- Microsoft Azure including the Microsoft Datacenters service, which manages datacenters, IaaS, and PaaS supporting services for the M365 Online Services (Delta) applications including hosting of servers, network support, authentication, virtual server hosting and system data storage, as well as M365, which provides supporting services to the M365 Online Services (Delta).
- M365 Central Services, which provides subscription-based access to a suite of online productivity applications and services for home and business use.

The M365 GRC team is responsible for identifying dependencies of each service and monitoring the organizations' implementation of agreed-upon security, availability, processing integrity, and confidentiality controls. Dependencies are documented in Inter-Service Agreements. Monitoring includes, but is not limited to, the review of third-party service auditor reports and discussions with subservice organization management. Note that M365 Online Services (Delta) considers Microsoft Azure, including Microsoft Datacenters, and M365 Central Services, are separate organizations within this report and are defined as such.

System Incidents

There were no significant system incidents identified that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the control objectives or (b) otherwise resulted in a significant failure in the achievement of the control objectives as of May 15, 2025.

A brief overview of the subservice organizations used by M365 Online Services (Delta) is below.

Organization	Brief Description
Microsoft Azure, including Microsoft Datacenters	Microsoft Azure's cloud Platform-as-a-Service (PaaS) offerings are used by M365 Online Services (Delta) to host production data and handle logical access and change management controls for M365 Online Services (Delta). Microsoft Datacenter's Infrastructure-as-a-Service (IaaS) offerings are used by M365 Online Services (Delta) to host physical and virtual servers and system data storage. Microsoft Datacenters also handles physical and environmental security controls for M365 Online Services (Delta).
M365 Central Services	M365 Online Services (Delta) uses M365 Central Services shared services and supporting technology to support the IT environment including logical access, server baselines, incident management, restoration of customer content, and vulnerability scanning.

Description of Control Objectives and Activities

Logical Access	
Control Objective 1	Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
Change Management	
Control Objective 2	Changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented consistent with management's intentions.
Data Redundancy	
Control Objective 3	Data redundancy controls exist to provide reasonable assurance that key information is replicated or backed up and can be restored in a timely manner.
Monitoring and Incident Management	
Control Objective 4	The security of the environment is monitored to provide reasonable assurance that security vulnerabilities are detected and remediated.
Network Services	
Control Objective 5	Control policies and procedures provide reasonable assurance that network devices are maintained to address the latest security and operational risks.
Physical Security	
Control Objective 6	Physical access to computer and other resources relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate personnel.

Logical Access

Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.

Identity Access Management

M365 owns and manages tools that regulate access to M365 production environments. Most service teams use the IDM access management service to limit access to authorized users. The service, managed by the Access Control team, allows each of the other service teams to manage their respective AD clusters for their respective environment. Several backend processes synchronize with other internal Microsoft tools, such as Microsoft HR department systems, to check that user information (e.g., employment status, manager, cost center, background check information) meets predefined requirements. Users who meet predefined criteria are able to request access to certain eligibilities, and access is only granted after approval.

New User or Modification of User Access

The process to request and approve new access via access management tools is managed through automated workflows configured within these tools. The systems automatically route access requests to the requestor's manager for approval. Users who meet specified requirements (e.g., active user, active manager, applicable cost center, or background check) can request specific access rights within each environment. User requests trigger notifications to the user's manager via email of a pending access request requiring manager approval. No access is provisioned within production environments until manager approval is obtained.

There are certain groups, roles, or entitlements that fall outside the automated provisioning processes described above. In each case users must still submit access requests, and each request must be approved before the access is manually provisioned.

External Users (Customer Entities) – When a new customer is added to the M365 service, they are provided with an initial account for system setup. The provisioning of users and deactivation of users is the responsibility of the customer entity.

Termination Access Removal

When individuals leave the company, Microsoft HR updates the terminated employees' details in the HR system, which syncs to access management tools via backend tasks. Access for terminated employees is then removed from respective service production environments. Without the appropriate entitlements, the user cannot access services within the M365 environment.

Periodic User Access Review

Services using the automated access provisioning processes above rely on workflows within the systems to automatically revoke user access based on the following criteria:

- *Inactivity* - after 35 days of inactivity, the user's account is disabled.
- *Manager Change* - when a user's manager and/or cost center has changed, users must re-request access using the same process described above, and the new manager must approve the user's requested access.
- *Group Predefined Expiration* - where applicable, services have security groups that have a set expiration period from when an account was granted access to the group.

Periodic reviews, both manual and automated, are conducted to verify that each user's access remains relevant and aligns with their job responsibilities. Some of these reviews use the automated M365 UAR Tool, while others are tracked manually by the services.

Just-in-Time Access

Just-in-time (JIT) tools allow individuals to request temporary elevated access privileges on an as-needed basis to limited areas within the respective service team's associated production environments.

Each tool follows a similar process before granting temporary elevated access to requesting engineers. Automated configurations within each tool notify the submitting user's manager with details of the access requested. If approved, the requesting user is granted access on a temporary basis, and the tool automatically removes the requested access based on built-in functionality within the tool. In certain cases, an engineer may receive a one-time preapproval for access elevations to specific areas within an environment; however, the access is still temporary in duration. Additionally, each elevation is logged and retained by the service team for incident evaluations.

Developer/Operations Model - Developer Access to Production

Using the access tools described above, the service teams have restricted access to appropriate personnel, including the enforcement of segregation between developers and operations personnel.

Select service teams allow developers temporary access to production using the JIT tools and approval processes described above. Developer access is limited to specific areas of the environment for deployment or operations purposes. These limitations are enforced using Torus, a Remote PowerShell tool. Torus allows for the restriction of access to specific commands that can be run in the service team's environment and requires approvals for each command being requested. The Torus request and approval process is managed by the JIT tools described above. For requests to make changes to production code or data by a developer or operator, an associated deployment request ticket must be provided and approved by a separate individual.

Background Checks

Backgrounds checks are required and renewed every 2 years for all full-time employees (FTE) and vendors internationally, as permitted by the laws of each country, before access is granted to certain eligibilities within each workstream.

Microsoft full-time employees request background checks, when necessary, through the OSP employee portal. A notification is sent to the requesting employee's manager for approval. If approved, a notification email is sent to Microsoft HR to process a background check for the requesting employee. When the background check is complete, HR enters the results into SAP.

For vendors and contractors, vendor companies are responsible for completing a valid background check for each contracted vendor. Once completed, Microsoft receives an attestation letter from the vendor company confirming the completion and pass status of the vendor's background check. Once the background check validation is received, Microsoft enters relevant information into SAP through the ECS interface. Background check information for FTEs and vendors is pushed from SAP to an IDM database, after which the IDM tool checks for employee background check information before access to M365 cloud environments can be requested by the employee. Full and incremental sync jobs run to keep the data used by the IDM tool current.

Service administrators configure requirements, including background check, for eligibilities within each workstream. If no background check is on file, or if a background check has expired, the user receives an error indicating that the employee does not have the required background check, thus preventing the employee or vendor from obtaining those eligibilities.

Authentication

Internal users are authenticated using Remote Desktop Services and must be authenticated using a two-factor authentication mechanism that includes a smartcard with PIN to log into the RDG. After logging in to the RDG, the user must enter his/her production account user ID and password to access production servers. The corporate

password requirements are defined and configured within code, and passwords are automatically generated. These requirements include password complexity, length, history, and duration. Additionally, internal users can gain temporary access to elevated roles allowing access to customer content via the JIT methods described above. For those services that only use JIT elevations to access the environment with no standing access, there are requirements built into the JIT tools for generating one-time complex passwords for authenticating into these environments.

External Users – Microsoft provides various options to enable the authentication mechanism for end users and M365 customers. Each external entity is responsible for substantiating that the mechanism is configured and operating, as well as enforcing the use of strong passwords.

Data Transmission (Encryption)

Encryption between Microsoft employee and datacenter connection

RDG connections are configured to establish Secure Socket Layer (SSL) connections between the internal users and the server. The SSL encryption algorithm is Federal Information Processing Standard (FIPS) 140 compliant.

Additionally, access to the M365 applications and support services environments by Microsoft employees to both the RDG and the service servers is encrypted using the defined encryption settings and protocols described above. This encryption is managed by the M365 Remote Access team.

Encryption between client and Microsoft datacenter connection

Based on the customer's data connection request, the encrypted connection is configured through the Microsoft network between the client and the desired M365 application and support services. The encryption levels are set by the customer, but each M365 service team has a specified and maintained listing of allowable encryption protocols that the customer may use.

Encryption between Microsoft datacenters

Each service team is responsible for establishing secured and encrypted connections across datacenters. Teams that use an Azure PaaS subscription rely on Azure to configure and manage encryption settings.

Data at Rest (Encryption)

Customer content at rest in the M365 environment is encrypted at rest utilizing full disk encryption or file level encryption. The data is encrypted through the use of BitLocker for disk level encryption and custom code built into the applications and supporting services for file level encryption. Additionally, teams that store data on Azure Blob storage utilize Azure's built-in encryption at rest.

Data Segregation

Customer content is stored and processed on a shared database, which is logically segregated using program logic and a different customer identifier.

Server Build-out Process

M365 has a defined server build-out process to deploy and configure new servers and rebuild existing servers. As part of the server build-out process, each service team performs the following:

- Connect the server to the specified domain.
- Install anti-malware agents to get up to date anti-malware signature files and definitions.
- Install a server agent to collect server activities and upload the logs to the Security Incident Response (SIR) team databases for security assessment activities.

After the base server image is applied and the related build-out process is finished, quality assurance reviews are conducted to validate that the server build-out process is completed as expected. The quality assurance review follows a process for server build-out compliance:

- Automated build-out tool:

  Application and supporting service teams that leverage an automated build-out and deployment process utilize a scan, which is performed by the deployment tool to substantiate the build had completed successfully. If there is a failure, the tool attempts to redeploy the build until successful.

Certain services leverage Microsoft's Azure PaaS offerings for server build-out and management. Teams who use Azure IaaS with customized server images maintain, update, and test server images as part of the deployment process. Once the server image has been tested, it is provided to Azure for actual deployment.

Change Management

Control Objective 2: Changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented consistent with management's intentions.

Service Infrastructure and Support Systems Change Management

Service and support related changes follow an established change management process for the M365 environment. Each change is tracked within identified ticketing systems, which contain information that can be linked to approval and testing details related to the change. These ticketing systems are listed in the *Software* section above. Appropriate authorizations and approvals needed for the changes being made to these environments are defined in the tickets.

When service teams or customer representatives enter a request for a change to the M365 environment in the change management systems, a representative of the relevant workstream is charged with addressing the change request. If a code modification is required, the addressor will perform a pull request, which replicates the master branch's code and allows the user to perform necessary code modifications without disrupting the live code running in production. Each individual change or addition made to address the change request is subject to a peer review in which another workstream representative reviews and approves the individual code changes. Once a change is peer reviewed and approved, it is checked into a build, along with other changes that are currently in the workstream's deployment process. Each build is subject to security and static analysis testing to test for the presence of security vulnerabilities. Except for in specific scenarios, M365 environment change management processes require a 100% testing pass rates prior to moving forward in the deployment process. When a build successfully completes security testing, it is deployed to preproduction environments for integration testing. Builds can be independently deployed to the preproduction environments or multiple builds can be aggregated into a "release," which is subject to integration testing. Code that has successfully completed all testing types is then deployed to the master code repository and is recognized as the newest version of the workstream's source code. There are generally three types of preproduction environments, or "rings," for ring validation integration testing:

- DogFood: The workstream's initial test ring, consisting of a subset of Microsoft employees and customers who test changes on Microsoft's behalf.
- MSIT: The MSIT ring allows the release to be subject to testing by all Microsoft employees.
- Slice in Production (SIP): Once the release is successfully integrated into the MSIT ring, it is moved into the SIP environment, which consists of about 5% worldwide customers who have decided to opt in and are able to provide feedback.

Certain types of changes in M365 change management systems are subject to additional review and approval processes dependent on the nature of the change. The four approval levels based on the nature and impact of the change have been included below:

- Auto-approval – A set of preapproved, low-risk standard changes.
- Functional (Peer) Approval – Standard changes with a slightly higher level of risk.
- Change Advisory Board Approval – Changes with the potential for high risk and high impact.
- Emergency Change Advisory Board Approval – A risk that must be remediated timely, such as an out of band security patch.

M365 service teams use a variety of tools to deploy changes to Azure. The ability to deploy code is restricted to appropriate build deployers using a combination of IDM, Torus, and Lockbox permissions.

Security Development Lifecycle

M365 environments follow the standard Microsoft Security Development Lifecycle (SDL) process which includes, at a minimum, risk assessment, testing, approval, and documentation. The SDL process includes security development requirements, which are intended to reduce the number of security-related bugs that appear in the design, code, and documentation associated with a software release, as well as to detect and remove those bugs as early in the SDL as possible.

Risk assessment and design review occurs in a Change Advisory Board entitled “Office Hours” whose members formally “Approve” or “Deny” any major or significant change prior to implementation. Members include representatives from Compliance, Security, and Microsoft Legal teams.

Testing, including code reviews, occurs during the development and build processes. Results of the tests, reviews, and approvals are tracked through ticketing systems used by each team. These ticketing systems are listed in the *Software* section above.

Data Redundancy

Control Objective 3: Data redundancy controls exist to provide reasonable assurance that key information is replicated or backed up and can be restored in a timely manner.

Data Replication and Data Redundancy

The M365 Online Services (Delta) defined in this report use Azure for data replication and data redundancy services. Where applicable, Azure performs replication and redundancy of customer content.

Business Continuity

The majority of M365 service teams participate in the Enterprise Business Continuity Management (EBCM) program that uses a common set of criteria to determine the relevancy and frequency of failover exercises. Teams not yet integrated into the EBCM process perform periodic failover testing. Where relevant, failover exercises are conducted on a regular basis to test applications and related data to verify the accessibility at a secondary disaster recovery location. The frequency of conducting failover exercises, as well as the recovery time objectives (RTOs) for each application and support service, are based on the nature and criticality of the systems. The RTOs are developed as part of the overall M365 Business Continuity and Disaster Recovery Planning. The primary objective of conducting failover exercises is to test whether the RTOs may be met in case of a disaster. Issues identified as part of the failover tests are tracked to ultimate resolution.

Control Objectives and Related Control Activities

The service organization remains responsible for the representations in the description of controls, as listed below. These control activities include preventive, detective, and corrective policies and procedures that help M365's Online Services (Delta) analyze, decrease, manage, and respond to risk in a timely manner.

The table below contains a listing of the control activities evaluated as part of this report, note that where a control activity is covered by one of the subservice organizations a reference to the subservice organization will be added. Further details on the coverage of the subservice organization will be described in Complementary Subservice Organization Controls (CSOC) section below, including the control activities and control areas (e.g., Redundancy, Network Security) covered by the subservice organizations.

Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.

Control Activities	Report Coverage Mapping
1.01 (CA-33.b): Elevated access within the M365 production environment is approved by an authorized user.	• M365 Online Services (Delta) • CSOC - M365 Central Report
1.02 (CA-34): Identity of users is authenticated to M365 Services. The use of passwords incorporates policy on periodic change and password complexity.	• M365 Online Services (Delta) • CSOC - M365 Central Report • CSOC - Microsoft Azure Report
1.03 (CA-35.b): Elevated access within the M365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis.	• M365 Online Services (Delta) • CSOC - M365 Central Report
1.04 (CA-36): Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.	• M365 Online Services (Delta) • CSOC - M365 Central Report
1.05 (CA-37): Each M365 Service customer's content is segregated from other Online Services customers' content to isolate customer tenant data flows.	• M365 Online Services (Delta) • CSOC - Microsoft Azure Report
1.06 (CA-44): Data in motion is encrypted when transmitting data between the customer and the data center and between data centers.	• M365 Online Services (Delta) • CSOC - Microsoft Azure Report

Complementary User Entity Control Considerations

- User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access.
- User entities establish proper controls over the use of system IDs and passwords.
- User entities are responsible for managing their users' password authentication mechanism.
- User entities enforce desired level of encryption for network sessions.
- User entities secure the software and hardware used to access M365.

Complementary Subservice Organization Controls Considerations

- M365 Central Services (Central Services Report) - M365 Central Services is responsible for maintaining controls that restrict and revoke access to the M365 environment based on employment status, manager approvals, and background check requirements. M365 Central Services is also responsible for enforcing data encryption, and baseline security configurations applied on servers deployed to production.
- Microsoft Azure (Microsoft Azure ("Azure") including Microsoft Datacenters Report) - Microsoft Azure is responsible for maintaining controls over access management (including authentication), change management, operational controls, and data protection to the platform services supporting M365. Additionally, for services using Azure, Azure is responsible for maintaining controls over:
  - Secure transmission, handling, and storage of data (including encryption, redundancy, replication, and recovery).
  - Security and incident management and vulnerability scanning for M365 services hosted on the Azure platform.

Control Objective 2: Changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented consistent with management's intentions.

Control Activities	Report Coverage Mapping
2.01 (CA-18): Changes and software releases within the M365 environment are documented / tracked and are approved prior to implementation into production.	• M365 Online Services (Delta)
2.02 (CA-20): Emergency changes to the production environment follow an emergency change approval process.	• M365 Online Services (Delta)
2.03 (CA-21): Testing is carried out on all changes according to established procedures. Users and stakeholders review and approve results of testing prior to implementation.	• M365 Online Services (Delta)
2.04 (CA-46): Production releases undergo a security review prior to their release into the production environment per defined criteria, including a code review.	• M365 Online Services (Delta)

Control Objective 3: Data redundancy controls exist to provide reasonable assurance that key information is replicated or backed up and can be restored in a timely manner.

Control Activities	Report Coverage Mapping
3.01 (CA-49): Procedures have been established for local redundant storage and/or other redundancy measures supporting the availability of applications and customer content.	• M365 Online Services (Delta) • CSOC - Microsoft Azure Report
3.02 (CA-51): Customer content and services are replicated to a geographically separate location.	• M365 Online Services (Delta) • CSOC - Microsoft Azure Report

Complementary Subservice Organization Controls Considerations

- M365 Central Services (Central Services Report) - M365 Central Services is responsible for maintaining restoration and retention controls for stored customer content.
- Microsoft Azure (Microsoft Azure ("Azure") including Microsoft Datacenters Report) - Microsoft Azure is responsible for maintaining controls over access management (including authentication), change management, operational controls, and data protection to the platform services supporting M365. Additionally, for services using Azure, Azure is responsible for maintaining controls over:
  - Secure transmission, handling, and storage of data (including encryption, redundancy, replication, and recovery).
  - Security and incident management and vulnerability scanning for M365 services hosted on the Azure platform.

Control Objective 4: The security of the environment is monitored to provide reasonable assurance that security vulnerabilities are detected and remediated.

CSOC – The security monitoring and incident management processes aligned with Control Objective 4 are wholly carved-out to the M365 Central Services Report and the Microsoft Azure Report.

Control Objective 5: Control policies and procedures provide reasonable assurance that network devices are maintained to address the latest security and operational risks.

CSOC – The network service processes aligned with Control Objective 5 are wholly carved-out to the Microsoft Datacenters, which is included in the Microsoft Azure Report.

Control Objective 6: Physical access to computer and other resources relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate personnel.

CSOC – The physical security processes aligned with Control Objective 6 are wholly carved-out to Microsoft Datacenters, which is included in the Microsoft Azure Report.

Complementary User Entity Controls (CUECs)

M365 Online Services (Delta) transaction processing and the controls over that processing, were designed with the assumption that certain controls are in operation within the user entity organizations. This section describes those controls that should be in operation at user entity organizations to complement the controls of M365 Online Services (Delta). The following list contains controls that M365 Online Services (Delta) assumes their user entities have implemented. User organization auditors should determine whether the user entities have established sufficient controls in these areas:

Complementary User Entity Controls	Relevant Control Objective
User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access.	Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
User entities establish proper controls over the use of system IDs and passwords.	Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
User entities are responsible for managing their user's password authentication mechanism.	Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
User entities enforce desired level of encryption for network sessions.	Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
User entities secure the software and hardware used to access M365.	Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.

Complementary Subservice Organization Controls (CSOCs)

Microsoft's controls related to the M365 Online Services (Delta) system detailed in this report cover only a portion of overall internal control for each user entity of M365 Online Services (Delta). It is not feasible for the control objectives related to M365 Online Services (Delta) to be achieved solely by Microsoft. The software in scope for this report has varying dependencies on Azure and M365 services that are covered in separate assurance reports. The responsibility of these subservice organizations is considered in the execution and evaluation of the controls. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with M365's controls, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as follows:

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant Control Objective
Logical Access, Baseline Servers, Data Encryption	M365 Central Services	M365 Central Services is responsible for maintaining controls that restrict and revoke access to the M365 environment based on employment status, manager approvals, and background check requirements. M365 Central Services is also responsible for enforcing data encryption, and baseline security configurations applied on servers deployed to production.	**Control Objective 1:** Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
Restoration of Customer Content	M365 Central Services	M365 Central Services is responsible for maintaining restoration and retention controls for stored customer content.	**Control Objective 3:** Data redundancy controls exist to provide reasonable assurance that key information is replicated or backed up and can be restored in a timely manner.
Security and Incident Management, Vulnerability Scanning	M365 Central Services	M365 Central Service is responsible for maintaining controls over the security and incident management and vulnerability scanning.	**Control Objective 4:** The security of the environment is monitored to provide reasonable assurance that security vulnerabilities are detected and remediated.

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant Control Objective
Platform as a Service (PaaS) Logical Access	Microsoft Azure, including Microsoft Datacenters	Microsoft Azure is responsible for maintaining controls over access management (including authentication), change management, operational controls, and data protection to the platform services supporting M365. Additionally, for services using Azure, Azure is responsible for maintaining controls over: • Secure transmission, handling, and storage of data (including encryption, redundancy, replication, and recovery). • Security and incident management and vulnerability scanning for M365 services hosted on the Azure platform.	Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted. Control Objective 3: Data redundancy controls exist to provide reasonable assurance that key information is replicated or backed up and can be restored in a timely manner. Control Objective 4: The security of the environment is monitored to provide reasonable assurance that security vulnerabilities are detected and remediated.

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant Control Objective
Infrastructure as a Service (IaaS) Physical Security	Microsoft Azure, including Microsoft Datacenters	Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities supporting M365, including datacenters. Additionally, Microsoft Datacenters is responsible for maintaining controls over: • Protection of the network environment, including perimeter firewalls, restricting access to network devices and monitoring network devices for compliance with security standards. • Physical access to the facilities, including data centers, supporting M365. • Environmental threats (including natural disasters and man-made threats). • Physical data storage, protection, and disposal services supporting M365.	Control Objective 5: Control policies and procedures provide reasonable assurance that network devices are maintained to address the latest security and operational risks. Control Objective 6: Physical access to computer and other resources relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate personnel.

Section 4:
Supplemental Information Provided by Management of Microsoft

Section 4:
Supplemental Information Provided by Management of Microsoft

The information included in this section is presented by Microsoft Corporation ("Microsoft") to provide additional information to user entities and is not part of Microsoft's description of the system. The information included here in this section has not been subjected to the procedures applied in the examination of the description of the system and, accordingly, Deloitte & Touche LLP expresses no opinion on it.

Business Continuity Planning

The Microsoft 365 ("M365") service incorporates resilient and redundant features in each service and utilizes Microsoft's enterprise-level datacenters. These datacenters use the same world-class operational practices as Microsoft's corporate line of business applications. The M365 team's long experience in operating highly available services, combined with the company's close ties to the product groups and support services, provides a comprehensive solution for the company's online services with the ability to meet the high standards of its customers.

The company's online services' designs include provisions to quickly recover from unexpected events such as hardware or application failure, data corruption, or other incidents that may affect a subset of the user population. The company's service continuity solutions and framework are based on industry best practice and are updated on a regular basis to support Microsoft's ability to recover from a major outage in a timely manner.

Domain Name Services

M365 Domain Name Service (DNS) provides authoritative name resolution for a subset of public-facing domains associated with M365. These domains can be purchased by customers to rename their domain URLs.

Datacenter Services

The Microsoft Datacenters Management team has overall responsibility for the oversight of datacenter operations, including physical security, site services (server deployments and break/fix work), infrastructure build-out, critical environment operations and maintenance, and facilities management. Site Security Officers are responsible for monitoring the physical security of the facility 24x7.

The Microsoft Datacenters Management team conducts periodic operational reviews with the key third-party vendors that support the Microsoft Datacenters. The purpose of the operational reviews is to discuss the current state of agreed-upon deliverables. Third-party vendors have specific statements of work with service level agreements that are monitored for compliance and adherence. Statements of work are reviewed on a periodic basis and updates are made accordingly, as business needs require.

ISO/IEC Standards 42001:2023, 27001:2022, ISO 27002:2022, 27017:2015, 27018:2019, 27701:2019, and 22301:2019

M365 is compliant with ISO standard 42001:2023 and meets the requirements of ISO 27001:2022, 27002:2022, 27017:2015, and 27018:2019, published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). M365 is also compliant with ISO standards 22301:2019 and 27701:2019.

ISO27000 series of standards were developed in the context of the following core principles:

"The preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required)."

M365 has been certified against the above standards by Mastermind (42001) and the British Standards Institute (BSI). To view the certificates, see the Certificate/Client Directory Search Results page located on the BSI Global website. Certificates are available for customers to download from the Microsoft Service Trust Portal.

NIST 800-53 and FISMA

M365 implements security processes and technology that adhere to the NIST 800-53 standards required by US federal agencies and have acquired FedRAMP Authority to Operate (ATO) from multiple federal agencies.

Cloud Service Continuous Improvements

M365 is a dynamic service, which Microsoft continually updates with the latest features and functionality. While new features and functionality are regularly being added, the risk-based controls applied to the new components are expected to remain consistent with the risk-based controls applied to the existing M365 suite of services.

Controls Not Subject to this Examination

Control Activity	Management's Response
(CA-20): Emergency changes to the production environment follow an emergency change approval process.	Cloud Input Intelligence (CII) No Occurrence - M365 management noted that there was no occurrence for this control for Cloud Input Intelligence (CII).