NOTICE: You and your company have obtained access to this report on the description of the system of Microsoft Corporation – Microsoft 365 Central Services ("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 Central Services ("M365"). 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 M365 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 M365.

This SOC 1 Report is intended only to be used by M365's existing clients during the period 10/1/2023, through 9/30/2024, and their external auditors (i.e., "user entities") during the period 10/1/2023, through 9/30/2024, and the "user auditors," 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 M365.

Deloitte & Touche, its subsidiaries and subcontractors, and their respective personnel have no responsibility for the description of the system of M365, 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 Central Services

System and Organization Controls (SOC) 1 Report

October 1, 2023, through September 30, 2024

This report, including the description of tests of controls and results in Section 4, is intended solely for the information and use of management of Microsoft, user entities of Microsoft's M365 Central Services system during some or all of the period October 1, 2023, to September 30, 2024, 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

Section 1: Independent Service Auditor’s Report 1

Section 2: Management of Microsoft’s Assertion 6

Section 3: Management of Microsoft’s Description of Its Microsoft 365 Central Services System 9

Section 4: Management of Microsoft’s Description of Its Control Objectives and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results 38

Section 5: Supplemental Information Provided by Management of Microsoft 59

Executive Summary

Microsoft Corporation— Microsoft 365	
Scope	Microsoft 365 (M365) Central Services
Period of Examination	October 1, 2023, through September 30, 2024
Location(s)	Redmond, WA
Subservice Providers	Yes – • Microsoft Azure (“Azure”) including Microsoft Datacenters
Opinion Result	Unqualified
Controls with Testing Exceptions	4
Complementary User-Entity Controls	Yes – See **Page 33**
Complementary Subservice Organization Controls	Yes – See **Page 35**

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 Central Services system ("M365") of Management of Microsoft Corporation (the "Service Organization" or "Microsoft") for processing user entities' transactions throughout the period October 1, 2023, to September 30, 2024, included in **Section 3**, "Management of Microsoft's Description of Its Microsoft 365 Central Services System" (the "Description") and the suitability of the design and the operating effectiveness 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 Central Services system that are not likely to be relevant to user entities' internal control over financial reporting.

The information in **Section 5**, "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 Central Services system made available to user entities during the period October 1, 2023, to September 30, 2024. Information in **Section 5** has not been subjected to the procedures applied in the examination of the Description of the M365 Central Services system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the Description of the M365 Central Services system and, accordingly, we express no opinion on it.

The Service Organization uses Microsoft Azure ("Azure") including the Microsoft Datacenters service ("subservice organization") for its hosting of physical and virtual servers, network management, data protection and storage services. 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 organization. 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 organization or their functions, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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 operating effectiveness 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 operating effectiveness 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 and operating effectively to achieve the related control objectives stated in the Description throughout the period October 1, 2023, to September 30, 2024. 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 operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness 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 or operating effectively to achieve the related control objectives stated in the Description.

- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the Description were achieved.

- 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 or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in **Section 4**, "Management of Microsoft's Description of Its Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results."

Emphasis of a Matter – Cyber Incident

Microsoft has publicly acknowledged cyberattacks by a state-sponsored entity known as Midnight Blizzard. Passwords and other secrets were exfiltrated, allowing access to certain source code repositories, additional secrets, databases, and applications. Microsoft acknowledged that certain passwords, secrets, and code repositories relevant to this report were accessed or exfiltrated. Microsoft represented that these passwords and secrets have been rotated or remediated. Microsoft also stated that code repository access gained by the threat actor was not and cannot be used to make production changes. We inspected certain listings provided by Microsoft of applications, resources, and code repositories impacted by these incidents, including those aligned to passwords and secrets that were accessed. We did not identify evidence that contradicts Microsoft's explanations and representations. Microsoft has determined that the incident was closed on October 15, 2024.

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 Central Services system that was designed and implemented throughout the period October 1, 2023, to September 30, 2024.

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 throughout the period October 1, 2023, to September 30, 2024, and subservice organization and user entities applied the complementary controls assumed in the design of Microsoft's controls throughout the period October 1, 2023, to September 30, 2024.

c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved, throughout the period October 1, 2023, to September 30, 2024, and if complementary subservice organization and user entity controls assumed in the design of Microsoft's controls operated effectively throughout the period October 1, 2023, to September 30, 2024.

Restricted Use

This report, including the description of tests of controls and results in **Section 4**, is intended solely for the information and use of management of Microsoft, user entities of Microsoft's M365 Central Services system during some or all of the period October 1, 2023, to September 30, 2024, 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

February 26, 2025

Section 2:
Management of Microsoft’s Assertion

Microsoft

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 Corporation's Assertion**

For the period from 10/1/2023 to 9/30/2024

We have prepared the description of the Microsoft 365 Central Services system ("M365") of Management of Microsoft Corporation (the "Service Organization" or "Microsoft") for processing user entities' transactions throughout the period October 1, 2023, to September 30, 2024, included in **Section 3**, "Management of Microsoft's Description of Its Microsoft 365 Central Services System" (the "Description"), for user entities of the system during some or all of the period October 1, 2023, to September 30, 2024, 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 the subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

The Service Organization uses Microsoft Azure ("Azure") including the Microsoft Datacenters service ("subservice organization") for its hosting of physical and virtual servers, network management, data protection and storage services. 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 organization. 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 organization.

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 Central Services system made available to user entities of the system during some or all of the period October 1, 2023, to September 30, 2024, 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, 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. Includes relevant details of changes to the service organization's system during the period covered by the Description.

c. 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 Central Services 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 operated effectively throughout the period October 1, 2023, to September 30, 2024, to achieve those control objectives if the subservice organization and user entities applied the complementary controls assumed in the design of Microsoft's controls throughout the period October 1, 2023, to September 30, 2024. 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.

   c. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Section 3:

Management of Microsoft’s Description of Its Microsoft 365 Central Services System

Section 3: Management of Microsoft's Description of Its Microsoft 365 Central Services System

Overview of Operations

Business Description

Microsoft Corporation's ("Microsoft") Microsoft 365 ("M365") service is 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.

Customers subscribe to a standard set of features and services which are hosted in a shared, multi-tenant environment. The Microsoft 365 Enterprise Cloud (M365) is a complete, intelligent solution designed for the needs of large and midsize organizations. It combines cloud-based applications with productivity services, including the latest Office applications, and a full suite of online services for Operating systems, email, file storage, collaboration, and meetings.

This includes the Government Community Cloud, an M365 offering designed for US government customers. Also included is the Government Community Cloud High and Department of Defense offering, in which customers subscribe to a standard set of features hosted in a multi-tenant environment designed for the US Federal government, defense industry, aerospace industry, and government contractors, to provide United States International Traffic in Arms Regulations (ITAR) support and meet Defense Information Systems Agency requirements.

Additionally, M365 is part of the Microsoft Cloud for Financial Services offering. Microsoft Cloud for Financial Services provides capabilities to manage data to deliver differentiated experiences, empower employees, and combat financial crime. It also facilitates security, compliance, and interoperability. This set of cloud-based solutions enhances collaboration, automation, and insights to streamline processes; personalizes every customer interaction; improves customer experience; and delivers rich data insights. The data model enables Microsoft's partners and customers to extend the value of the platform with additional solutions to address the financial industry's most urgent challenges. These capabilities will help organizations align to business and operational needs, and then deploy quickly to accelerate time to value Microsoft Cloud for Financial Services. Its capabilities (Unified Customer Profile, Customer Onboarding, and Collaboration Manager) are built atop Azure, Microsoft Dynamics 365, Microsoft Power Platform, and Microsoft 365 offerings. Azure, Microsoft Dynamics 365, and Microsoft Power Platform are not part of the scope of this report.

M365 is physically hosted in Microsoft-managed datacenters. Microsoft Datacenters is an organization within Microsoft, that provides hosting and network support solutions for the M365 environment. Microsoft Azure ("Azure") is an organization within Microsoft that provides supporting services for the M365 applications including authentication, virtual server hosting, and system data storage and protection. Microsoft Datacenters is managed and run by Azure and both services 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 audited separately and therefore are not within the scope of this report.

The following services are provided to all M365 customers:

- Email access and productivity tools
- Team communication and collaboration
- Document and other file storage

- Documents viewed and edited in a Web browser
- Hosted Operating systems
- Intelligent Platform features

M365 streamlines workflow for customers by providing them with added security, increased email accessibility, and easy team collaboration by providing hosted messaging and collaboration solutions.

Applicability of the Report

This report has been prepared to provide information on M365's 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 software offerings described in the sections below.

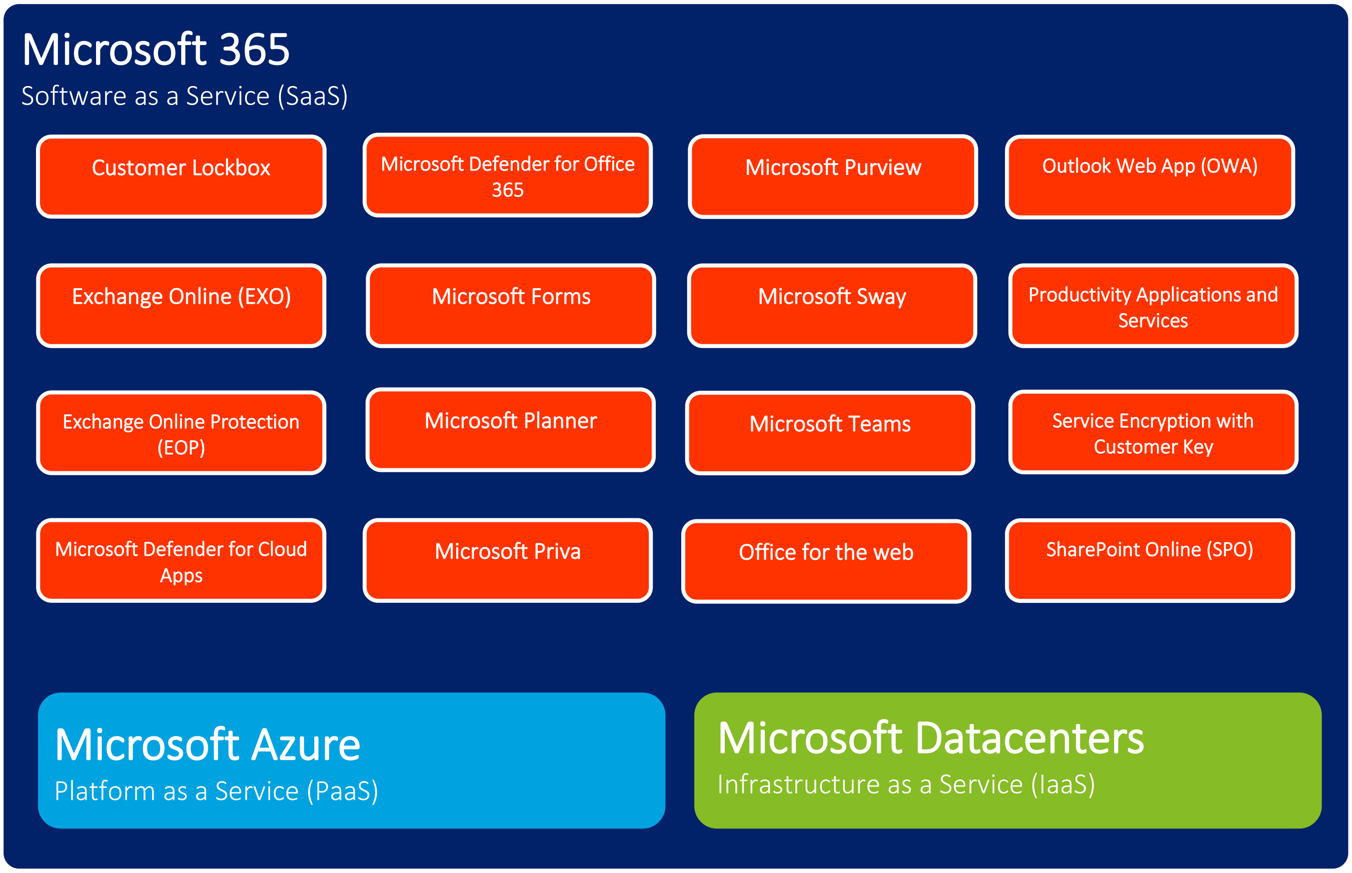
Infrastructure

All M365 services are hosted on a combination of the following subservice organizations within Microsoft: Microsoft Datacenters Infrastructure as a Service (IaaS) and Azure's IaaS and Platform as a Service (PaaS).

For Microsoft Datacenters hosting, the physical servers are owned by M365, the operating system (OS) and software are managed by M365, and network layer and network layer protections are implemented by 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 configuration 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 PaaS provides customer authentication and rights management services through Microsoft Entra ID (formerly Azure Active Directory (AAD)). The controls managed by Microsoft Datacenters and Azure are audited separately and therefore not in the scope of this report.


Microsoft 365
Software as a Service (SaaS)
Customer Lockbox
Microsoft Defender for Office 365
Microsoft Purview
Outlook Web App (OWA)
Exchange Online (EXO)
Microsoft Forms
Microsoft Sway
Productivity Applications and Services
Exchange Online Protection (EOP)
Microsoft Planner
Microsoft Teams
Service Encryption with Customer Key
Microsoft Defender for Cloud Apps
Microsoft Priva
Office for the web
SharePoint Online (SPO)
Microsoft Azure
Platform as a Service (PaaS)
Microsoft Datacenters
Infrastructure as a Service (IaaS)

Software

M365 includes the following SaaS offerings:

- Customer Lockbox – An access control technology designed to provide customer control and transparency over access to customer content.
- Exchange Online (EXO) – An email service.
- Exchange Online Protection (EOP) – A service providing security features, such as antivirus, antimalware, and antispam filtering for Exchange.
- Microsoft Defender for Cloud Apps – A service providing security features supporting the M365 internal and external services, including App Governance.
- Microsoft Defender for Office 365 – A cloud-based service designed to protect against email threats like phishing, business email compromise, and malware. Key features include Advanced Hunting, Attack Simulation, and Training, and One Cyber endpoint protection. The service offers tools for investigation, hunting, and remediation to help security teams manage threats efficiently.
- Microsoft Forms – Create surveys, quizzes, and polls with real-time results, built-in response analytics, and export to Excel.
- Microsoft Planner – Provides a visual way to organize teamwork with simplified task management.
- Microsoft Priva – A service that provides personal data protection, automated privacy risk mitigation, and management of subject rights requests at scale.
- Microsoft Purview – A family of data governance, risk, and compliance solutions that helps organizations govern, protect, and manage their entire data estate. The following Microsoft Purview solutions are

included within the scope of this report: Auditing, Communication Compliance, Compliance Manager, Data Lifecycle Management, Records Manager, Data Loss Prevention, eDiscovery, Information Protection, Unified Feedback Platform, Insider Risk Management, Data Classification Services, Exact Data Match, and ML Inference.

- Microsoft Sway – Digital storytelling application for creating interactive reports, presentations, personal stories, and more.
- Microsoft Teams – A communication service that offers a threaded persistent chat experience that builds on M365's group infrastructure, global scale, enterprise grade security, and graph driven intelligence. Microsoft Teams is also referred to as Azure Communication Service (ACS).
- Office for the web (formerly known as Office Online) - Enables users to view and edit Word, Excel, PowerPoint, OneNote, and Visio documents online via a web browser.
- Outlook Web App (OWA) – A web client for accessing Microsoft 365 email.
- Productivity Applications and Services –
    - Tasks – Business Scenario Service – A service supporting extensibility scenarios within the Tasks platform through a common API.
- Service Encryption with Customer Key – A service providing customers with two application-level encryption options for customer content at rest within the Exchange and SharePoint environments: Service Encryption with Microsoft-owned encryption keys and Service Encryption with customer-owned encryption keys ("Customer Keys").
- SharePoint Online (SPO) – A solution for creating websites to share documents and information with colleagues and customers. This information and documentation repository includes OneDrive, Microsoft 365 Backup, and Project Online. This also includes Viva Topics, a unified knowledge and content experience across M365 and Viva Connections, which provides a personalized destination for employees to discover other Viva applications, relevant news, conversations, and the tools they need to succeed.

M365 uses the following to support the above offerings:

- Microsoft 365 (M365) Remote Access – A set of servers providing remote access to M365 service production environments via authorized two-factor authentication and encryption.
- Identity Manager (IDM) – An access management service providing an integrated and broad solution for managing M365 user identities and associated credentials for all M365 services (with the exception of some service teams which also leverage OneIdentity through the Azure offering).
- Intelligent Conversation and Communications Cloud (IC3) – A supporting service for Microsoft Teams service allowing first-party real-time conversation products including audio and video calling, meetings, and chat services.
- Office Services Infrastructure (OSI) – A platform for backend applications including deployment, hosting, and monitoring infrastructure applications.
- Vanquish - Internal service providing security monitoring and intrusion detection for M365 services.
- Substrate Intelligence Platform (SIP) – A secure platform that enables M365 product teams to train and deploy intelligent features.
- Containers on Substrate Managed Intelligent Clusters (Cosmic) – A non-customer facing internal M365 capability that provides a centralized and standard mechanism for service teams to deploy their Azure-based applications and containers to meet the M365 business compliance policies.

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.
- CorpFIM/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, 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 the 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 (excluding some service teams that utilize OneIdentity through the Azure offering).
- 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 and redundancy 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 OneIdentity.
- Azure – Provides customer authentication infrastructure including Microsoft Online Directory Services, Microsoft Organization ID, and Microsoft Entra ID (formerly AAD).
- Microsoft 365 Remote Access – Provides internal users remote access control and authentication to the M365 environment.

Procedures

M365 adheres to Microsoft Corporation's Security Policy, which is owned by the Information Risk Management Council (IRMC), comprised of business and security leaders across the company, and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) for Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses:

- Human resources security
- Asset management
- Access 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, transfers in, stores 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 trainings periodically in order to design, build, and operate secure cloud services.

Microsoft 365 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. These 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 includes 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, 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 uses Microsoft Azure ("Azure") including the Microsoft Datacenters service, which manages datacenters, IaaS, and PaaS supporting services for the M365 applications including hosting of servers, network support, authentication, virtual server hosting and system data storage. Note that M365 considers Azure and Microsoft Datacenters as two separate organizations within this report and are defined as such.

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.

A brief overview of the subservice organizations used by Microsoft 365 is below.

Organization	Brief Description
Microsoft Azure	Microsoft Azure's cloud Platform-as-a-Service (PaaS) offerings are used by M365 to host production data and handle logical access and change management controls for M365.
Microsoft Datacenters	Microsoft Datacenters' Infrastructure-as-a-Service (IaaS) offerings are used by M365 to host physical and virtual servers and system data storage. Microsoft Datacenters also handles physical and environmental security controls for M365.

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 one or more of those control objectives during the period October 1, 2023 to September 30, 2024.

Significant Changes

There were no changes that are likely to affect report users' understanding of how the system is used to provide the service since the last issued report covering the period ended September 30, 2023. Please see the Software section above for details over the in-scope services.

Description of Control 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.
Customer Lockbox	
Control Objective 5	Controls provide reasonable assurance that customer content is only accessed when authorized by a designated customer account administrator.
Service Encryption with Customer Key	
Control Objective 6	Controls provide reasonable assurance customer mailboxes are encrypted using customer keys, data that is deleted per request is no longer accessible, and customers data is isolated to those with access to the appropriate customer key.

Logical Access

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

Overview

Background Checks

Backgrounds checks are required and renewed every 2 years for all full-time employees 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 required background check, thus preventing the employee or vendor from obtaining those eligibilities.

Identity Access Management

Microsoft 365 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 can request access to certain eligibilities, and access is only granted after approval.

Some access is regulated outside the IDM service via other tools and processes; however, the functionality and processes are the same. These tools include IDWeb and OneIdentity.

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 the 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 to 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 employee’s 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 56 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 Pre-defined 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.

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 onetime 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 Management

Data Segregation

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

Customer Lockbox

Control Objective 5: Controls provide reasonable assurance that customer content is only accessed when authorized by a designated customer account administrator.

For customers utilizing the Customer Lockbox feature, Customer Lockbox is an access control technology included in M365, designed to provide customer control and transparency over access to customer content hosted in Microsoft datacenters. The service grants Microsoft engineers temporary access to customer content on as-needed basis only as approved by an appropriate tenant authority. The following sections, prefixed with "Customer Lockbox," detail the procedures in place to limit Microsoft access to customer generated content.

Customer Lockbox - Authorization and Notification

Access to customer content for customers utilizing the Customer Lockbox feature is initiated through a Service Request made via Microsoft's customer support. If the Service Request requires access to customer content, the access is requested through the Customer Lockbox tool. Individuals who are approved to access the customer content do so using the Remote PowerShell (RPS) tool.

Only Microsoft engineers with appropriate access entitlements within the Exchange environment, can request temporary elevation to the 'AccessToCustomerData' role, which allows access to customer content. The request process is built into Customer Lockbox. If approved by the role owners, Microsoft managers, the request is then routed to a customer contact for additional approval.

Customer Lockbox - Customer Approval

The automated workflows supporting the Customer Lockbox elevation process require that elevation requests are first approved by Microsoft management before being submitted to a tenant administrator. Tenant administrators are assigned and are the responsibility of each customer. If the request is not approved within a specified period of time by both the Microsoft management and the tenant administrator, then the elevation request times out and becomes invalid.

Customer Lockbox - Associated Service Request

Each elevation request made using Customer Lockbox must reference an associated service request number before submission to Microsoft management for approval. Attempts to submit an elevation request without an associated service request number will fail, and the RPS tool will return an error. Service requests are either submitted by the effected customer or created and communicated to the customer prior to the elevation request.

Customer Lockbox - Microsoft 365 Admin Center

M365 customers can review a history of Customer Lockbox elevation requests within the customer's M365 Admin Center. The history includes relevant information for current and past elevation requests, including the date, service request number, duration of elevation, reason for elevation, and requestor. The logs are kept for a reasonable period of time.

Customer Lockbox - Searchable Audit Logs

Server activity is logged for each Customer Lockbox elevation, and the activity log repository is available to each Customer Lockbox customer. Activity logs show what actions and commands were executed on a server containing customer content by a Microsoft engineer for the time allowed during an elevation requested through Customer Lockbox.

Customer Lockbox - Management Review of Elevations

Microsoft management pulls logs of Customer Lockbox elevations, as well as capacity server administrator elevations, from a data repository and investigates any anomalies. Any anomalies identified are discussed and actioned in a weekly service review. The statistics are aggregated and reviewed annually with Microsoft management. For customers who have chosen to use Customer Lockbox, it is the only way to access customer content. Any other access paths are considered malicious access and are not covered by this attestation.

Service Encryption with Customer Key in Microsoft 365

Control Objective 6: Controls provide reasonable assurance customer mailboxes are encrypted using customer keys, data that is deleted per request is no longer accessible, and customers data is isolated to those with access to the appropriate customer key.

For customers utilizing the Service Encryption with Customer Key feature, Microsoft 365 provides customers with two application level encryption options for their data within Exchange and SharePoint service: 1) Service Encryption with Microsoft owned encryption keys, and 2) Service Encryption with customer-owned keys (“Customer Keys”).

In the standard Microsoft Service Encryption described above, M365 owns the encryption keys for the customer’s Exchange mailboxes and SharePoint sites. Service Encryption with Customer Key (“Customer Key”) is an opt-in encryption offering that allows M365 customers to supply and manage their own encryption keys for advanced, self-managed protection. The Customer Key offering is available in both the Exchange Online Worldwide, GCC-M, GCC-H, Department of Defense environment, as well as the SharePoint Online Worldwide environment.

Each “Customer Key” subscription a customer maintains has its own service tenant encryption identifier, and two corresponding Azure-hosted customer key vaults. The customer keys are housed in Azure Key Vault; the onboarding process is inclusive of an Azure subscription creation, which customers will then use to house their keys which correspond with their “Customer Key” service. The two respective Azure Key Vaults each maintain a unique encryption key provided by the customer during the “Customer Key” onboarding process.

For EXO: The “Customer Key” model can be applied to all users within a customer’s AD environment or can be segregated based on customer preferred user groupings or business unit differentiations. Each respective Exchange “Customer Key” subscription instance maintains its own Data Encryption Policy (“DEP”) that must be configured by the customer admin during the onboarding process as well. Once a DEP has been created, the customer can provision AD user mailboxes to that DEP, applying that encryption policy to the user mailboxes provisioned to that Customer Key DEP.

For SPO: The Customer Key model is applied at the tenant level via Tenant Intermediate Keys "TIKs"; if a customer opts-in to Customer Key, all SharePoint site instances are encrypted at the application layer.

Customer mailboxes or SharePoint sites associated with a Customer Key DEP or TIK are only accessible through utilizing the customer root keys relevant to each encryption policy type, which are stored in Azure Key Vault. Through Azure, Microsoft maintains its own interim keys, but an interim key does not have the ability to decrypt customer data. Under rare circumstances, Microsoft may need to access resources with customer content to perform specific service oriented and maintenance tasks.

To do this the service performs a customer key wrap operation, in which Microsoft’s interim key is sent to Azure blob storage to be wrapped with a data blob of the customer key. The Azure key wrap function does not allow Microsoft access to the unique customer root keys themselves; the interim keys are instead wrapped with the root key data for access purposes. Once retrieved, the Microsoft engineer can access resources with customer data to perform the relevant service tasks. Once the tasks are complete, an unwrap operation is performed, in which the wrapped interim key is sent to Azure blob storage to be unwrapped and consequently disassociated from the customer root key housed in Azure Key Vault. Unwrapped interim keys cannot access Customer Key encrypted data.

Microsoft provides additional protections if the customer owned root keys are lost or stolen with an “Availability Key”, which provides M365 customers with the capability to recover from the unanticipated loss of root keys. Microsoft will either assist customers through this process or provide customers with instructions on how to recover without assistance from Microsoft.

The Availability Key is a root key that is provisioned and protected by Microsoft and is functionally equivalent to the root keys that are supplied by the customer for use with service encryption with “Customer Key.” Because the Availability Key is protected by Microsoft, it uses a different security design and controls from keys that the customer manages. This provides defense-in-depth and protects against the loss of all keys from a single attack or point of failure. Sharing the responsibility to protect the keys, while using a variety of protections and processes for key management, ultimately reduces the risk that all keys will be lost or destroyed.

Service Encryption with Customer Key in Microsoft 365 – Termination

Customers can opt out of the Service Encryption with Customer Key service. For EXO, customers can revoke root key access, either through group divestiture at a DEP level or through full-service exit. Since the TIK applies to all SharePoint instances, opting out of the Customer Key service consequently applies to all of the tenant's SharePoint instances.

When a tenant wishes to opt-out of the Service Encryption with Customer Key service, the Exchange and SharePoint tenant administrators must confirm that the customer is truly opting out of the service and wants the data to be deleted. Once a customer opts-out of the service, deletes their own root keys, and signs the eDocument stating their service termination, Microsoft locks the customer out of their data as a confirmation step that the tenant would truly like that data to be deleted. Once this step has been taken, the customer's executive team must formally communicate the opt-out decision on behalf of the customer via signed and notarized documentation. Microsoft will maintain their root key to the customer's data until the executive confirmation of service termination has been received, or the 90- to 180-day deletion period threshold has been reached. Once the customer service termination confirmation has been communicated, the customer can request that Microsoft delete its root key access to the data in question.

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 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

Data for customer content, applications and support services is replicated for redundancy and disaster recovery purposes. M365 applications and supporting services are generally replicated from the primary content database to a secondary content database within the same primary datacenter. The primary and secondary databases are then replicated across geographically dispersed datacenters. Generally, the data maintained in the primary content database is replicated and accessible in real time via: (1) the primary database; (2) a secondary replication database located in the same primary datacenter with real time data; (3) a secondary disaster recovery server with real time replicated data in a geographically segregated datacenter; or (4) a server with a few minutes lag replication in a geographically dispersed datacenter.

Data is accessible for redundancy and disaster recovery purposes for applications and support services through the data replication process described above, to meet the SLA requirements.

It should be noted that the replication process described above reflects the processes in place for the EXO and SPO systems at an overall level. The supporting service teams perform similar replication processes, such as utilizing an Active-Active (e.g., EOP) replication process, but do not maintain lag copies of data. Azure based services rely on Azure capabilities for geo-redundant replication and storage.

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.

Customer Termination

Customer content is retained after termination of M365 subscriptions per agreed upon commitments with the customer in the contract and SLAs. Customers are responsible for the upload/download and management of data stored within the M365 environments related to confidentiality.

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.

Vulnerability and Patch Management

The M365 Security team monitors for known configuration and patching vulnerabilities through automated scans based on Qualys technology. A master server is configured to scan each server across the M365 applications and supporting services suite to analyze and report known vulnerabilities and patch non-compliance. Each service team reviews the vulnerability scan report from the master server and assesses the criticality of the vulnerabilities and applies patches as applicable.

New vulnerabilities (e.g., those from responsible disclosure programs) are communicated to M365 through the Microsoft Security Response Center. If a patch is developed for the vulnerability, each service team evaluates the relevance of the patch to its environment and applies the patch as applicable.

Security Incident Monitoring

M365 has implemented incident response procedures, which consist of technical mechanisms, organizational infrastructure, and other procedures to detect, respond, and deter security incidents. The M365 incident management technical infrastructure includes monitoring systems for detecting and alerting M365 personnel of security events and incidents. A monitoring agent is installed on each server at the time of server build-out to transfer the security logs to the Security Incident Response (SIR) team, which identifies potential incidents and serves as a central repository for investigations. Incidents posing significant risk to the environment are prioritized for response and mitigation.

Additionally, each service team has on-call personnel covering a 24/7 schedule. If an incident is assigned a high enough severity, applicable contingency plans are invoked. When a contingency plan is invoked, the incident manager on shift works with the M365 Security team to implement the contingency plan.

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 antimalware agents to get up to date antimalware 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 completed as expected. The quality assurance review follows a process for server build-out compliance:

- <u>Automated build-out tool:</u>

  Application and supporting service teams that leverage an automated build-out and deployment process utilize a scan 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.

Control Objectives and Related Control Activities

The control objectives and related control activities are documented in **Section 4** to reduce the redundancy that would result from listing them in this section and repeating them in **Section 4**. The control objectives and related control activities are however an integral part of the description of the system. While listed in **Section 4**, the service organization remains responsible for the representations in the description of controls. These control activities include preventive, detective, and corrective policies and procedures that help M365 identify, decrease, manage, and respond to risk in a timely manner.

Complementary User Entity Control Considerations (CUECs)

Microsoft 365 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. The following list contains controls that M365 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
CUEC-01: 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.
CUEC-02: 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.
CUEC-03: 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.
CUEC-04: 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.
CUEC-05: User entities manage anonymous access to SPO sessions.	**Control Objective 1:** Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
CUEC-06: 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.
CUEC-09: User entities are responsible for enabling and maintaining email restoration for EXO.	**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.
CUEC-08: User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.	**Control Objective 4:** The security of the environment is monitored to provide reasonable assurance that security vulnerabilities are detected and remediated.
CUEC-15: When employing Customer Lockbox, user entities are responsible for reviewing Microsoft requests to customer content, and approving appropriate requests in a timely manner.	**Control Objective 5:** Controls provide reasonable assurance that customer content is only accessed when authorized by a designated customer account administrator.
CUEC-16: User entities subscribing to the Service Encryption with Customer Keys service who use customer-owned keys are responsible for importing or generating their own encryption keys.	**Control Objective 6:** Controls provide reasonable assurance customer mailboxes are encrypted using customer keys, data that is deleted per request is no longer accessible, and customers data is isolated to those with access to the appropriate customer key.

Complementary User Entity Controls	Relevant Control Objective
CUEC-17: User entities subscribing to the Service Encryption with Customer Keys service who use customer-owned keys are responsible for restricting access to the Azure Key Vault subscription.	**Control Objective 6:** Controls provide reasonable assurance customer mailboxes are encrypted using customer keys, data that is deleted per request is no longer accessible, and customers data is isolated to those with access to the appropriate customer key.
CUEC-18: User entities subscribing to the Service Encryption with Customer Keys service who use customer-owned keys are responsible for rotating customer managed keys per their compliance policies.	**Control Objective 6:** Controls provide reasonable assurance customer mailboxes are encrypted using customer keys, data that is deleted per request is no longer accessible, and customers data is isolated to those with access to the appropriate customer key.

Complementary Subservice Organization Controls (CSOCs)

Microsoft's controls related to the M365 system detailed in this report cover only a portion of overall internal controls for each user entity of M365. It is not feasible for the control objectives related to M365 to be achieved solely by Microsoft. The software in scope for this report have varying dependencies on Azure services that are covered in a separate assurance report. The responsibility of this subservice organization 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
Platform as a Service (PaaS) Logical Access	Microsoft Azure	Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting M365.	**Control Objective 1:** Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
Platform as a Service (PaaS) Change Management	Microsoft Azure	Microsoft Azure is responsible for maintaining controls over the deployment of changes to M365 production environments.	**Control Objective 2:** Changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented consistent with management's intentions.
Redundancy and Restoration of Customer Content	Microsoft Azure	Microsoft Azure is responsible for maintaining controls over the restoration, redundancy, and retention of 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.
Operating System Configurations	Microsoft Azure	Microsoft Azure is responsible for maintaining controls over base operating system images, including security configurations and monitors, applied to servers deployed to M365 production environments.	**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
Network Device Management	Microsoft Datacenters	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.	N/A – Network Services is wholly carved-out to Microsoft Datacenters.
Infrastructure as a Service (IaaS) Physical Security	Microsoft Datacenters	Microsoft Datacenters is responsible for maintaining controls over physical security of datacenters supporting Azure and M365.	N/A – Physical Security is wholly carved-out to Microsoft Datacenters.

Section 4:
Management of Microsoft’s Description of Its Control Objectives and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results

Section 4: Management of Microsoft's Description of Its Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results

Description of Testing Procedures Performed

Deloitte & Touche LLP performed a variety of tests relating to the controls listed in this section throughout the period from October 1, 2023, through September 30, 2024. Our tests of controls were performed on controls as they existed during the period of October 1, 2023, through September 30, 2024, and were applied to those controls specified by Microsoft.

In determining the nature, timing, and extent of tests, we considered (a) the nature and frequency of the controls being tested, (b) the types of available evidential matter, (c) the assessed level of control risk, (d) the expected effectiveness of the test, and (e) our understanding of the control environment.

In addition to the tests listed below, we ascertained through multiple inquiries with management and the control owner that each control activity listed below operated as described throughout the period. Tests performed are described below:

Test	Description
Corroborative Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control during the report period to evidence application of the specific control activity.
Examination of documentation/Inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Reperformance of monitoring activities or manual controls	Obtained documents used in the monitoring activity or manual control activity, independently reperformed the procedures, and compared any discrepancies identified with those identified by the responsible control owner.
Reperformance of programmed processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

Testing of Tools Supporting Control Activities

For the tools used in the performance of control activities in **Section 4**, we performed procedures to address the risks associated with their use. While these procedures were not specifically included in the test procedures listed in **Section 4**, they were completed as part of the testing to support our conclusions.

Reliability of Information Produced by the Service Organization

We performed procedures to evaluate whether the information provided by the service organization, which includes (a) information in response to ad hoc requests from the service auditor (e.g., population lists); and (b) information used in the execution of a control (e.g., exception reports or transaction reconciliations), was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Our procedures to evaluate whether this information was sufficiently reliable included procedures to address (a) the accuracy and completeness of source data and (b) the creation and modification of applicable report logic and parameters. While these procedures were not specifically called out in the test procedures listed in this section, they were completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by the Service Organization.

Reporting on Results of Testing

The concept of materiality is not applied when reporting the results of control tests because Deloitte & Touche LLP does not have the ability to determine whether an exception will be relevant to a particular user entity. Consequently, Deloitte & Touche LLP reports all exceptions.

Logical Access

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

Control Activity	Tests Performed	Test Result
CA-33.a (1.01) - Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources.	• Inquired of Logical Access control owners and ascertained that an automated process has been established for requesting and approving access prior to access being granted to user eligibilities. • Obtained and inspected source code of the system configurations within the identity access management tool to corroborate that access requests or modifications for users require approval. Additionally, for a sample eligibility, observed that approval was obtained prior to access being granted. • Obtained and inspected access eligibility documentation for all in-scope applications to ascertain that a request for access is required to be submitted and authorized prior to granting any users access.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-33.b (1.02) - Elevated access within the M365 production environment is approved by an authorized user.	• Inquired of Logical Access control owners that processes have been established for requesting and approving access prior to access being granted. • Observed and inspected the system configurations for elevated access within the M365 production environment to ascertain that elevated access is restricted to only approved individuals and is limited based on the established time constraints (for Just in Time Systems). • For Just in Time Systems - Observed for a sample of one user per just in time system that the individual was approved prior to access being elevated, and that the access duration was limited to the requested time. • For the IDM System - Obtained and inspected logs of access changes for administrators during the examination period. Observed no new administrators were granted access during the examination period.	Identity Manager (IDM) No Occurrence All Other Services No Exceptions Noted
CA-34 (1.03) - Identity of users is authenticated to M365 Services. The use of passwords incorporates policy on periodic change and password complexity.	• Inquired of Logical Access control owners that authentication processes and password policies are enforced. • Observed system configuration settings for a selected server for each service to ascertain that authentication polices regarding change intervals and complexity are being enforced.	Exchange (EXO) and Microsoft Teams Exception Noted. For 1 sampled server selected for testing, local password paraments were not configured according to a centralized policy. All Other Services No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-35.a (1.04) - Access to privileged accounts is configured to be revoked automatically based on access expiration settings, including inactivity and Manager / Cost Center changes.	• Inquired of Logical Access control owners that processes have been established for identity access management system configuration to revoke access automatically based on account expiration settings, including inactivity, and Manager / Cost Center changes. • Obtained and inspected source code of the system configurations within the identity access management tools to corroborate that account expiration settings, including inactivity, and Manager / Cost Center changes are configured to remove access. Additionally, obtained and inspected the sync jobs for the settings to validate user data is periodically refreshed with HR Systems. • Obtained and inspected system logs and tracking details for selected individuals that expiration settings were enforced, and access was removed based on the configurations within the identity access management system.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-35.b (1.05) - Elevated access within the M365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis.	• Inquired of Logical Access control owners that processes have been established for reviewing elevated access that is not automatically expired. • Obtained and inspected user access review documentation for selected quarters to ascertain that access was reviewed, and any identified issues were addressed in a timely manner.	Identity Manager (IDM) Exception Noted. In 1 of the quarterly user access reviews selected for testing, the review of administrators was not done timely. Outlook Web App (OWA) Exception Noted. In the quarterly user access reviews selected for testing, 1 security group was not included. Exchange Online Protection (EOP), Microsoft Defender for Cloud Apps, Microsoft Defender for Office 365, Microsoft Priva, and Microsoft Purview Exception Noted. 2 users were removed untimely from the groups of Microsoft Priva and Attack Simulation. Further, an incomplete population of users was reviewed in Q2 and Q3. Exchange Online (EXO), Productivity Applications and Services, Microsoft Forms, Microsoft Planner, Microsoft Sway, Office for the web, and Substrate Intelligence Platform (SIP) Exception Noted. An incomplete population of users was reviewed in Q2 and Q3. Microsoft Teams Exception Noted. Internal Audit (IA) noted that for Microsoft Teams, 2 security groups were not reviewed during Q1. Further, an incomplete population of users was reviewed in Q2 and Q3. All Other Services No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-36 (1.06) - Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.	• Inquired of Logical Access owners to gain an understanding of how authentication is enforced, and processes established with relation to encrypting communication with the production environment. • Observed authentication to a selected production server to corroborate that two-factor authentication was required. • Obtained and inspected source code configurations and system settings corroborating the encryption settings enforced for accessing the production environment.	No Exceptions Noted
CA-43 (1.07) - When users no longer require access or upon termination the user access privileges are revoked in a timely manner.	• Inquired of Logical Access control owners to gain an understanding of the process for disabling or removing access in a timely manner. • Compared a listing of all terminated/ transferred users within the examination period with active user accounts in the M365 environments to ascertain if access for terminated/ transferred employees was revoked. • Obtained and inspected HR termination reports for a selection of M365 terminated users to ascertain that removals of terminated users were executed in a timely manner by comparing the users' termination dates against the date of access revocation.	Exception Noted. 5 of 25 samples were not removed timely.
CA-37 (1.08) - Each M365 Service Customer's content is segregated from other Online Services customers' content to isolate customer tenant data flows.	• Inquired of Security process owners to gain an understanding of the processes that enforce logical segregation of customer content. • Obtained and inspected a sample of server configurations and, where applicable, tested user interfaces to ascertain that customer content is segregated.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-08 (1.09) - The M365 Service group works with Microsoft Human Resources and vendor companies to perform a background check on new or transferred personnel worldwide, where permitted by law before they are granted access to the M365 production assets containing customer content.	• Inquired of Governance, Risk & Compliance (GRC) process owners that new and transferred applicable employees and contractors are required to undergo a background check prior to being granted access to the environment. • Obtained and inspected automation that enforces background check requirement on eligibilities that grant access to production assets. • Obtained and inspected background check data for a selection of Microsoft personnel to ascertain that a background check was performed prior to granting access to the production assets containing customer content.	No Exceptions Noted

Complementary User Entity Control Considerations

- CUEC-01 - User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access.
- CUEC-02 - User entities establish proper controls over the use of system IDs and passwords.
- CUEC-03 - User entities are responsible for managing their user's password authentication mechanism.
- CUEC-04 - User entities enforce desired level of encryption for network sessions.
- CUEC-05 - User entities manage anonymous access to SPO sessions.
- CUEC-06 - User entities secure the software and hardware used to access M365.

Complementary Subservice Organization Control Considerations

- CSOC-01 - Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting M365.

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.

Control Activity	Tests Performed	Test Result
CA-03 (2.01) - Senior Management, as part of its major system release planning process, considers its commitments and requirements for Security, Availability, Confidentiality, and Processing Integrity.	• Inquired of Governance, Risk & Compliance (GRC) process owners to ascertain that Senior Management considers its commitments and requirements related to security, availability, confidentiality, and processing integrity as part of its major system release planning process. • Obtained and inspected evidence of the annual review including memorandums and planning meeting records, to ascertain that commitments and requirements for security, availability, confidentiality, and processing integrity were considered and approved by Senior Management, and these commitments and requirements were communicated to relevant personnel as part of the major system release planning process.	No Exceptions Noted
CA-18 (2.02) - Changes and software releases within the M365 environment are documented / tracked and are approved prior to implementation into production.	• Inquired of Change Management control owners that procedures have been established and are followed prior to deploying changes to the production environment. • Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that deployed changes are documented and tracked within a tracking tool. • Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that deployed changes were approved by appropriate stakeholders prior to release.	No Exceptions Noted
CA-20 (2.03) - Emergency changes to the production environment follow an emergency change approval process.	• Inquired of Change Management control owners that deployed emergency changes are approved by identified key stakeholders prior to release into production. • For the relevant services, obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that emergency changes were approved by identified key stakeholders.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-21 (2.04) - Testing is carried out on all changes according to established procedures. Users and stakeholders review and approve results of testing prior to implementation.	• Inquired of Change Management control owners that testing of changes is documented and required for deployment into production. • Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that changes are tested prior to release according to established procedures. • Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that testing was reviewed and approved prior to release according to established procedures.	No Exceptions Noted
CA-46 (2.05) - Production releases undergo a security review prior to their release into the production environment per defined criteria, including a code review.	• Inquired of SDL security process owners to ascertain that changes undergo a security review prior to release. • Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that a security review was performed prior to release for each build.	No Exceptions Noted
CA-19 (2.06) - For teams utilizing the Developer / Operations model, monitoring processes or system configurations are in place to identify and remediate unapproved changes to production.	• Inquired of Change Management and Logical Security control owners that for the teams using the Developer / Operations model, restrictions are in place to monitor or limit access to implement unapproved changes. • For the relevant services, observed that monitoring is in place for developers with access to the environment. • For the relevant services, obtained and inspected source code and change ticketing systems to ascertain that system configurations and procedures were in place to identify and remediate unapproved changes.	No Exceptions Noted

Complementary User Entity Control Considerations

- None.

Complementary Subservice Organization Control Considerations

- CSOC-11 - Microsoft Azure is responsible for maintaining controls over the deployment of changes to M365 production environments.

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.

Control Activity	Tests Performed	Test Result
CA-49 (3.01) - Procedures have been established for local redundant storage and/or other redundancy measures supporting the availability of applications and customer content.	• Inquired of Data Redundancy and Restoration process owners that processes have been established for data redundancy and restorations. • Obtained and inspected evidence for a selection of replications to ascertain that data redundancy and replication were occurring according to defined procedures and alternative data/application instances were available for restoration or failover.	No Exceptions Noted
CA-50 (3.02) - Service teams participate in Business Continuity programs, which specify, based on criticality, recovery objectives, testing requirements (up to full data center failover), and remediation timelines.	• Inquired of Business Continuity process owners to ascertain that failover tests occur on a regular basis. • Obtained and inspected business continuity documentation and failover logs for a selection of failover tests to ascertain that the tests were completed as designed, and that any issues identified were assigned to an appropriate owner and being tracked to resolution.	No Exceptions Noted
CA-51 (3.03) - Customer content and services are replicated to a geographically separate location.	• Inquired of Data Redundancy and Restoration process owners to gain an understanding of the process for locating customer content or services on replicated instances in geographically separate locations. • Obtained and inspected system configurations and depending on the setup of the service, a selection of data sources, to ascertain that replicated instances reside in geographically separate locations.	No Exceptions Noted

Complementary User Entity Control Considerations

- **CUEC-09** - User entities are responsible for enabling and maintaining email restoration for EXO.

Complementary Subservice Organization Control Considerations

- CSOC-12 - Microsoft Azure is responsible for maintaining controls over the restoration, redundancy, and retention of customer content.

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.

Control Activity	Tests Performed	Test Result
CA-26 (4.01) - Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked in an incident tracking system.	• Inquired of Monitoring and Incident management process owners that processes for identifying, reporting, and responding to security incidents have been established. • Obtained and inspected evidence for a selection of incidents to ascertain that identified security incidents were documented within an incident tracking system and resolved. • Inquired of Monitoring and Incident management process owners that processes for addressing security incidents have been established and include processes for escalation and review. • Obtained and inspected evidence for a selection of incidents to ascertain that security incidents were escalated and reviewed by the appropriate team and required action was taken.	No Exceptions Noted
CA-47 (4.02) - Security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures.	• Inquired of Monitoring and Incident management process owners that processes for identifying, reporting, and responding to security incidents have been established. • Obtained and inspected incident documentation for a selection of incidents to ascertain that identified security incidents were documented within an incident tracking system and resolved. • Inquired of Monitoring and Incident management process owners that processes for addressing security incidents have been established and include processes for escalation and review. • Obtained and inspected incident documentation for a selection of incidents to ascertain that security incidents were escalated and reviewed by the appropriate team and required action was taken.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-27 (4.03) - There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to ensure timely resolution of incidents of non-compliance.	• Inquired of Monitoring and Incident management process owners that processes for security vulnerability scanning have been established and outline requirements for addressing identified issues. • Obtained and inspected security scanning reports for a selection of servers for evidence that patches and vulnerability scans were being performed and completed successfully. • Obtained and inspected a sample of management reviews to ascertain that scan results were being reviewed and issues noted were being tracked to resolution.	Exception Noted. For 4 out of 25 samples of open port/network security group alerts, the alerts were not resolved timely. Further, for the Microsoft Purview service, Internal Audit (IA) identified 39 overdue alerts.
CA-38 (4.04) – Physical production servers go through a quality assurance review prior to installation in the production environment to confirm the server is configured in compliance with baseline security and operational settings according to the server's intended use.	• Inquired of Server Build-out management process owners that processes have been established to have baseline security and operational settings applied to all new servers deployed to the production environment. • Obtained and inspected system logs, source code configurations, and system change documentation for a selection of new servers to ascertain that baseline builds have been established, approved, and deployed prior to a new server being implemented in production.	Microsoft 365 Remote Access No Occurrence All Other Services No Exceptions Noted

Complementary User Entity Control Considerations

- **CUEC-08** - User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.

Complementary Subservice Organization Control Considerations

- CSOC-13 - Microsoft Azure is responsible for maintaining controls over base operating system images, including security configurations and monitors, applied to servers deployed to M365 production environments.

Customer Lockbox

Control Objective 5: Controls provide reasonable assurance that customer content is only accessed when authorized by a designated customer account administrator.

Control Activity	Tests Performed	Test Result
CA-56 (5.01) - Customer tenant administrators are automatically notified when a Customer Lockbox elevation request is initiated to access their content. The tenant administrator must authorize the access elevation request prior to access being granted to the content.	• Inquired of Operations and Security process owners to ascertain that Customer tenant administrators are notified when a Customer Lockbox elevation request is initiated to access their content. • Obtained and inspected system configurations within the identity access management tool to corroborate that elevation requests generate a notification and require approval prior to access being granted. • Observed for a selected Customer Lockbox subscriber, that a Lockbox request was submitted and approved by tenant management.	No Exceptions Noted
CA-57 (5.02) - Customer Lockbox elevation requests require management approval prior to submission to the tenant administrator.	• Inquired of Operations and Security process owners to ascertain that Customer Lockbox elevation requests require management approval prior to submission to the tenant administrator. • Obtained and inspected an access elevation log request and noted approvers were assigned to the request. Additionally, obtained and inspected system configurations within the identity access management tool to corroborate elevation requests require management approval prior to submission to the tenant administrator. • For a selected request, obtained and inspected access elevation logs to ascertain that an approval took place before access was granted.	No Exceptions Noted
CA-58 (5.03) - Customer Lockbox elevation requests to customer content require an associated service request.	• Inquired of Operations and Security process owners to ascertain that Customer Lockbox elevation requests to customer content require an associated service request. • Observed that for an elevation request when a service request number was excluded, the elevation request failed to be processed.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-59 (5.04) - Customer Lockbox elevation requests are displayed in the tenant M365 Admin Center.	• Inquired of Operations and Security process owners to ascertain Customer Lockbox elevation requests are displayed in the tenant M365 Admin Center. • Observed the population of Lockbox requests within the M365 Dashboard – Admin Center.	No Exceptions Noted
CA-60 (5.05) - When using Customer Lockbox, the service where the content is accessed logs the access made by the Microsoft Operator, and the entry can be found in the Audit log search.	• Inquired of Operations and Security process owners to ascertain that all servers that host customer content push audit logs to a repository on a real-time basis. • Observed for a sample elevation log that elevation activity was logged accordingly. • Observed for a sample elevation that it was identifiable through the M365 Dashboard search functionality.	No Exceptions Noted
CA-61 (5.06) - Microsoft management reviews both Customer Lockbox and capacity server elevation logs and investigates any anomalies. All elevations statistics are aggregated, reviewed, and reported to management annually.	• Inquired of Operations and Security process owners to ascertain that management reviews both Customer Lockbox and capacity server elevation. • Obtained and inspected a sample of the annual presentation which included elevation statistics and resolutions.	No Exceptions Noted

Complementary User Entity Control Considerations

- **CUEC-15** - When employing Customer Lockbox, user entities are responsible for reviewing Microsoft requests to customer content, and approving appropriate requests in a timely manner.

Complementary Subservice Organization Control Considerations

- None.

Service Encryption with Customer Key

Control Objective 6: Controls provide reasonable assurance customer mailboxes are encrypted using customer keys, data that is deleted per request is no longer accessible, and customers data is isolated to those with access to the appropriate customer key.

Control Activity	Tests Performed	Test Result
CA-62 (6.01) – Customer mailboxes are encrypted per customer's defined encryption policies using keys generated and maintained by the customer.	• Inquired with the Customer Key owners to ascertain that each customer is responsible for initiating their service encryption configuration during the Customer Key onboarding process. • Inquired with Customer Key owners to ascertain that each customer 'Customer Key' subscription has a unique service encryption identifier and a unique Azure Key Vault to house their root encryption keys. • Obtained and inspected a sample customer 'Customer Key' subscription and ascertained that each of the customer's service encryptions was associated with unique Azure Key Vaults for the respective encryption root keys.	No Exceptions Noted
CA-63 (6.02) – When a customer requests a key deletion using the Exchange Customer Key service, the data is no longer accessible by Microsoft or the end user.	• Inquired with the Customer Key owners to ascertain that once a customer opts out of the service and deletes their own root keys, all users associated with that tenant will no longer be able to log in to see the data. • Observed a test occurrence of a customer's Customer Key subscription termination process within the production environment to ascertain the customer data was no longer accessible after the tenant's termination of the Customer Key subscription.	No Exceptions Noted
CA-64 (6.03) – Only keys noted in the tenant's Data Encryption Policy can be used to access the data maintained in that tenant's service encryption.	• Inquired with the Customer Key owners to ascertain that data associated with a Customer Key Data Encryption Policy can only be accessed using the Data Encryption Policy 's Customer Keys. • Observed a test occurrence of a failed customer attempt to access an Azure Key Vault that was not associated with their 'Customer Key' service Data Encryption Policy.	No Exceptions Noted

Complementary User Entity Control Considerations

- CUEC-16 - User entities subscribing to the Service Encryption with Customer Keys service who use customer-owned keys are responsible for importing or generating their own encryption keys.
- CUEC-17 - User entities subscribing to the Service Encryption with Customer Keys service who use customer-owned keys are responsible for restricting access to the Azure Key Vault subscription.
- CUEC-18 - User entities subscribing to the Service Encryption with Customer Keys service who use customer-owned keys are responsible for rotating customer managed keys per their compliance policies.

Complementary Subservice Organization Control Considerations

- None.

Section 5:
Supplemental Information Provided by Management of Microsoft

Section 5: 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 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 27001:2022, 27017:2015, 27018:2019, 27701:2019, and 22301:2019

M365 is compliant with ISO standard 27001:2022 and meets the requirements of ISO 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 27702:2019.

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 the British Standards Institute (BSI). To view the certificates, see the Certificate/Client Directory Search Results page located on the BSI Global website.

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.

Microsoft 365 Copilot

Microsoft 365 Copilot is an advanced AI-powered assistant integrated into the Microsoft 365 suite. It leverages machine learning and natural language processing to assist users in various tasks, enhancing productivity and efficiency. It operates within the secure M365 environment. The Microsoft 365 Copilot service is included in the scope of the M365 Microservices SOC 2, Type 1 report, which is available for download via Microsoft's Service Trust Portal.

Management's Response to Exceptions Identified

The table below contains Management's responses to the exceptions identified in **Section 4**.

Control Activity & Exception	Management's Response
CA-27 - There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to ensure timely resolution of incidents of non-compliance. Exception Noted. For 4 out of 25 samples of open port/network security group alerts, the alerts were not resolved timely. Further, for the Microsoft Purview service, Internal Audit (IA) identified 39 overdue alerts.	Resolution of alerts can be delayed due to reviews, monitoring or service changes. To avoid closing bugs prematurely, we ensure that issues are thoroughly resolved and stable before marking them as closed. For Microsoft Purview, due to a reporting issue, less than 1% of nodes handling data classification and indexing did not report to the scanning service. However, 99.75% of compute nodes were properly configured and reported correctly.

Control Activity & Exception	Management's Response
CA-34 - Identity of users is authenticated to M365 Services. The use of passwords incorporates policy on periodic change and password complexity. Exchange (EXO) and Microsoft Teams Exception Noted. For 1 sampled server selected for testing, local password paraments were not configured according to a centralized policy.	While teams didn't use the centralized policy, they did create a custom policy for their environment which worked in conjunction with the JIT elevation and approvals for secure access to the servers. These servers do not allow interactive local user accounts to be provisioned.
CA-35.b - Elevated access within the M365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis. Identity Manager (IDM) Exception Noted. In 1 of the quarterly user access reviews selected for testing, the review of administrators was not done timely. Outlook Web App (OWA) Exception Noted. In the quarterly user access reviews selected for testing, 1 security group was not included. Exchange Online Protection (EOP), Microsoft Defender for Cloud Apps, Microsoft Defender for Office 365, Microsoft Priva, and Microsoft Purview Exception Noted. 2 users were removed untimely from the groups of Microsoft Priva and Attack Simulation. Further, an incomplete population of users was reviewed in Q2 and Q3. Exchange Online (EXO), Productivity Applications and Services, Microsoft Forms, Microsoft Planner, Microsoft Sway, Office for the web, and Substrate Intelligence Platform (SIP) Exception Noted. An incomplete population of users was reviewed in Q2 and Q3. Microsoft Teams Exception Noted. Internal Audit (IA) noted that for Microsoft Teams, 2 security groups were not	Logs of account usage have been reviewed and it was confirmed that there was no inappropriate access. Applicable teams have been reminded of this control requirement.

Control Activity & Exception	Management’s Response
reviewed during Q1. Further, an incomplete population of users was reviewed in Q2 and Q3.	
CA-43 - When users no longer require access or upon termination the user access privileges are revoked in a timely manner. Exception Noted. 5 of 25 samples were not removed timely.	For 3 samples, managers unfamiliar with the HR termination process did not submit termination data on time in the HR systems. To address this issue, M365 Leadership will collaborate with HR Leadership to ensure M365 managers are properly educated on termination procedures. For 2 samples, we have communicated the matter to M365 Leadership, and they are implementing additional monitoring.