Microsoft Corporation—Microsoft 365 Microservices (Type 1)

System and Organization Controls (SOC) 2 Report

September 30, 2023

Deloitte.

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 Microservices (Type 1) System 9

Section 4: Supplemental Information Provided by Management of Microsoft 85

Executive Summary

Microsoft Corporation— Microsoft 365 Microservices (Type 1)	
Scope	Microsoft 365 Microservices (Type 1)
Period of Examination	As of September 30, 2023
Locations	Redmond, WA
Subservice Providers	Yes: • Microsoft Azure (“Azure”) including Microsoft Datacenters • Microsoft 365 (“Central”)
Opinion Result	Unqualified
Complementary User-Entity Controls	Yes – See **Page 30**
Complementary Subservice Organization Controls	Yes – See **Page 32**

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 Microsoft 365 Microservices (Type 1) system[1] of Management of Microsoft Corporation (the "Service Organization" or "Microsoft" included in Section 3, "Management of Microsoft's Description of Its Microsoft 365 Microservices (Type 1) System" as of September 30, 2023 based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report*, in AICPA *Description Criteria* ("description criteria") and the suitability of the design and implementation of controls stated in the description as of September 30, 2023, to provide reasonable assurance that Microsoft's service commitments and system requirements would be achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality ("applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

The information in Section 4, "Supplemental information provided by Management of Microsoft," is presented by management of Microsoft to provide additional information and is not a part of management of Microsoft's Description of its M365 Microservices systems made available to user entities as of September 30, 2023. Information in Section 4 has not been subjected to the procedures applied in the examination of the Description of the M365 Microservices systems and of the suitability of the design and implementation of controls to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria and, accordingly, we express no opinion on it.

The Service Organization uses Microsoft Azure including the Microsoft Datacenter service for its hosting of physical and virtual servers, network management, and data protection and storage services. Additionally, Microsoft uses M365 Central shared infrastructure, as the services listed within the scope of this report are built upon the M365 Central infrastructure and will be included as part of the overall M365 service subscription ("subservice organizations"). The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Microsoft, to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria. The Description presents Microsoft's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Microsoft's controls. The Description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description indicates that complementary user entity controls that are suitably designed and operating

[1] In-scope services are defined in the Software subsection in Section 3 of this SOC 2 Report. These in-scope services are referred to throughout this report as "M365 Microservices." Items relating to the overall Microsoft 365 service will be referred to as "M365."

effectively are necessary, along with controls at Microsoft, to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria. The Description presents Microsoft's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Microsoft's controls. 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 controls.

Service Organization's Responsibilities

Management of Microsoft is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Microsoft's service commitments and system requirements would be achieved. Management of Microsoft has provided the accompanying assertion in Section 2 titled "Management of Microsoft's Assertion" (the "assertion") about the description and the suitability of the design and implementation of controls stated therein. Management of Microsoft is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of design and implementation of controls 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) 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, 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, the Description is presented in accordance with the description criteria, and the controls stated therein were suitably designed to provide reasonable assurance that Microsoft's service commitments and system requirements would be achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the Description is not presented in accordance with the description criteria and that controls were not suitably designed.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the Description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

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 report users and therefore may not include every aspect of the system that each individual report user may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design and implementation of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

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

Opinion

In our opinion, in all material respects,

a. The Description presents Microsoft's M365 Microservices (Type 1) system that was designed and implemented as of September 30, 2023 in accordance with the description criteria.

b. The controls stated in the Description were suitably designed as of September 30, 2023 to provide reasonable assurance that Microsoft's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of September 30, 2023 and if the subservice organizations and user entities applied the complementary controls assumed in the design of Microsoft's controls as of September 30, 2023.

Restricted Use

This report is intended solely for the information and use of management of Microsoft, user entities of the in-scope services for Microsoft's M365 Microservices as of September 30, 2023, business partners of Microsoft subject to risks arising from interactions with Microsoft's system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by Microsoft.
- How Microsoft's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how they interact with related controls at Microsoft to achieve Microsoft's commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use Microsoft's services.

- The applicable trust services criteria.
- The risks that may threaten the achievement of Microsoft's service commitments and system requirements and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

Deloitte & Touche LLP

January 23, 2024

Section 2:
Management of Microsoft's Assertion

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

Section 2: Management of Microsoft's Assertion

Microsoft Corporation's Assertion

As of September 30, 2023

We have prepared the description of the Microsoft 365 Microservices (Type 1) system[2] of Microsoft Corporation ("Microsoft" or the "Service Organization") included in Section 3, "Management of Microsoft's Description of Its Microsoft 365 Microservices (Type 1) System", as of September 30, 2023 (the "Description") based on the criteria for a description of a service organization's system in DC Section 200, 2018 *Description Criteria for a Description of a Service Organization's System in a SOC 2 Report,* in AICPA *Description Criteria*, ("description criteria"). The description is intended to provide users with information about our system that may be useful when assessing the risks arising from interactions with Microsoft's system, particularly information about system controls that Microsoft has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality ("applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

The Service Organization uses Microsoft Azure including the Microsoft Datacenter service for its hosting of physical and virtual servers, network management, data protection and storage services. Additionally, Microsoft uses M365 Central shared infrastructure, as the services listed within the scope of this report are built upon the M365 Central infrastructure and will be included as part of the overall M365 service subscription ("subservice organizations"). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Microsoft for Microsoft 365 Microservices, to achieve Microsoft's service commitments and system requirements related to Microsoft 365 Microservices based on the applicable trust services criteria. The description presents Microsoft's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Microsoft's controls. The description does not disclose the actual controls at the subservice organizations. The Description does not extend to controls of the subservice organizations.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Microsoft, to achieve Microsoft's service commitments and system requirements related to Microsoft 365 Microservices based on the applicable trust services criteria. The description presents Microsoft's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Microsoft's controls. The Description does not extend to controls of the user entities.

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

a. The description presents Microsoft's system that was designed and implemented as of September 30, 2023, in accordance with the description criteria.

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

b. The controls stated in the description were suitably designed and implemented as of September 30, 2023 to provide reasonable assurance that Microsoft's service commitments and system requirements related to the Microsoft 365 Microservices would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Microsoft's controls as of September 30, 2023.

Section 3:
Management of Microsoft's Description of Its Microsoft 365 Microservices (Type 1) System

Section 3: Management of Microsoft's Description of Its Microsoft 365 Microservices (Type 1) System

Overview of Operations

Business Description

Microsoft Corporation's (Microsoft) Microsoft 365 Microservices' (Type 1) systems[3] are components of Microsoft 365 (M365), a subscription-based business software service hosted by Microsoft and sold directly, or with partners, to various customers worldwide. Microsoft M365 services are designed to provide performance, scalability, security, management capabilities, and service levels required for mission-critical applications and systems used by business organizations. The scope of this SOC 2 Type 1 attestation is limited to controls covering the Microservices systems; however, due to how these systems are hosted within M365's environment, we deemed it necessary to also include a description of those aspects of M365's environment that directly support the Microservices.

The Microsoft 365 subscription offering comprises many services. Customer-facing and critical services, including Exchange, SharePoint, Microsoft Teams, and Office Online, are tested as part of the M365 Central reports. This M365 Microservices Type 1 report includes several backend processes, features, and other supporting infrastructure that are part of the M365 subscription but do not offer equally critical functionality as services included in the Central reports. Therefore, these services are separately presented in this SOC 2 Type 1 report.

M365 is physically hosted in Microsoft-managed datacenters. 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 not within the scope of this report. Microsoft Datacenters, Azure, and M365 Central services are treated as subservice organizations that are audited separately and therefore are not within the scope of this report.

The M365 Microservices rely on different functions of the M365 Central services, including but not limited to Security and Incident Management, Vulnerability Scanning, and Network Device Management.

Applicability of The Report

This report has been prepared to provide information on M365 Microservices' 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.

[3] In-Scope services are defined in the *Software* subsection in Section 3 of this SOC 2 Report. These in-scope services are referred to throughout this report as "M365 Microservices." Items relating to the overall Microsoft 365 service will be referred to as "M365."

This report covers the following M365 applications and related support services:

- Aesir
- Audio Enhancement (OMG)
- Bing Teams
- Bookings Odata API (Outlook)
- Compliance Drive
- Cortana
- Data Classification Services (DCS)
- Exchange Admin Center (EAC)
- IDEAs Delivery Service (IDS)
- Kevlar for Windows / Kevlar for Linux
- Microsoft 365 (M365) Security and Compliance Center (SCC)
- OMAHA
- Outlook Diagnostics
- Productivity Applications and Services
- Profile Data Roaming Service (PDRS)
- Project for the web
- Remote Help
- Suite User Experience (SUE)
- To Do
- Unified Feedback
- Viva Glint
- Viva Pulse
- Whiteboard Service

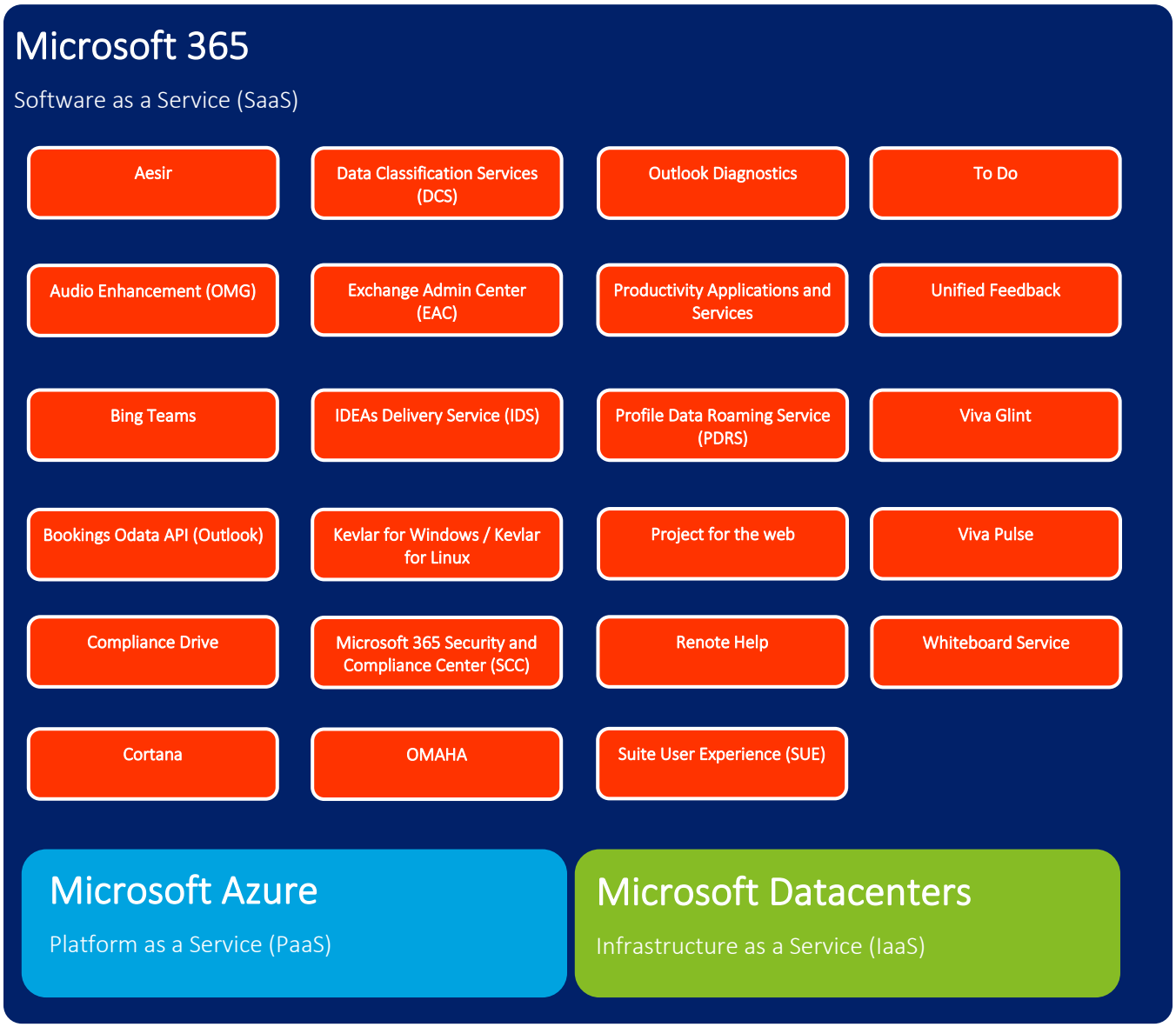
Infrastructure

All M365 Microservices 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 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 Azure Active Directory (AAD). The controls managed by Microsoft Datacenters, Azure, and M365 are audited separately and therefore are not within the scope of this report.



Software

M365 Microservices includes the following service offerings:

- Aesir – A set of common infrastructure for managing compute resources (including Delve, Hauk, and Thor). Delve is an M365 application where users can manage their M365 Profile and also discover and organize M365 content that's likely to be most interesting to them right now. Hauk is an API to access data. Thor is a set of APIs that power workplace search experiences across M365 services.
- Audio Enhancement (OMG) – A M365 service which provides Noise Suppression capabilities to the M365 product Microsoft Stream.
- Bing Teams – A set of M365 related services that perform various integrations within M365 and with the overall Bing service. These Bing Teams services are Falcon, Microsoft Search in Bing, QueryRewriting/Speller, and XAP.

- Bookings Odata API (Outlook) – A service that assists in organizing scheduled meetings and managing appointments across M365 services.
- Compliance Drive – A service that processes requests to read and write forensic evidence data for a given user. This service is utilized by the Microsoft Purview Insider Risk Management solution.
- Cortana – An enterprise productivity assistant which will process over Microsoft 365 data (such as emails, files, chats, and calendar items) to fulfill the user's request. The conversation platform consists of core platform services plus "skill" services which are tailored to fulfill specific types of queries. Cortana skills include: Alarms, Assistant Conversation, Audio Service, Bing Answers, Calendar Skill, Cortex, Device Control Skills, Email Skill in Hosting Service (formerly called Email Skill Cohosted with Cortex), Federated Search Bot, File Answer Skill, Grammar API, ILDC Voice Skills, Lists, MSAI Meeting Intelligence, New Eligibility API, Reminders, Semantic Machines, Skill Hosting Service, Teams Files Voice Skill, Teams Navigation Voice Skill, Teams Search & Polite Refusal Skill, Timers, UX Orchestrator, and Windows Skills.
- Data Classification Services (DCS) – A platform service for detecting sensitive information in user content. DCS is utilized by the Microsoft Purview Information Protection, Microsoft Purview Insider Risk Management, and Microsoft Purview Communication Compliance solutions.
- Exchange Admin Center (EAC) – A Web-based management console for managing Exchange. Designed to provide an experience that is more aligned with the overall Microsoft 365 admin experience.
- IDEAs Delivery Service (IDS) – Enables secure bulk-email sending capabilities via Azure Communication Services (ACS) and an integration with Exchange Online. The service uses DomainKeys Identified Mail (DKIM) standards to provide email authentication for spam mitigation while also providing telemetry that covers email delivery, bounces, views, and clicks.
- Kevlar for Windows / Kevlar for Linux – A non-customer facing internal M365 services that facilitate the Kevlar Compliance Pack on both Windows and Linux operating systems, a group of standard baseline M365 security and operational components, that each M365 service team can utilize and apply to their code change deployments (during the change management process) in order for the code change to meet the standardized M365 business compliance policies before it is deployed into the respective team's production environment.
- Microsoft 365 (M365) Security and Compliance Center (SCC) – A UI portal for administrators to configure and review Security and Compliance Features. This portal is utilized by the Microsoft Purview, Microsoft Priva, and Microsoft Defender for Office solutions.
- OMAHA – A data transfer tool used within M365.
- Outlook Diagnostics – A support services for Exchange.
- Productivity Applications and Services – A collection of services that enhance and augment the features in the Office clients. Experiences include: Augmentation Loop, Customer Content Pipeline, Designer App Service, Loop, M365 Apps Admin Portal, M365 Apps Inventory and Health, M365 App Management and Deployment, Admin Controlled Messaging Service, Captions, Client Telemetry (Nexus), Config, Discovery, Enrichment, Entity, Conversion (Excel, PowerPoint, and Word), Hubble Content and Media, Identity, ImageAnalysis, ImageToDoc, Insert Media, Insights, Language Experiences (Translation), Licensing, MRO Device Manager, Natural Language Editor, Office Augmentation, Office PowerPoint Mobius, Office TextAnalysis, PowerPoint Broadcast, PowerPoint Creator, PowerPoint Suggestion (Designer), Rendering (PowerPoint and Word), Recent Docs, Redirection, Roaming, Scripts, Shredder, Tasks – Business Scenario, TellMe, Templates, One Customer Voice (Feedback), One Survey Service, and Reply At-Mention.
- Profile Data Roaming Service (PDRS) (formerly Activity Feed Service) – A cloud platform service used to synchronize data across devices.

- Project for the web – Provides simple and powerful, cloud-based work management capabilities for project managers and team members to plan and manage work of any size.
- Remote Help – A cloud-based remote assistance solution that enables help desk connections within a tenant, including strong authentication and security, role-based access controls, device compliance checks, and session reporting.
- Suite User Experience (SUE) – The customer web portal for M365 websites and a web graphical user interface (GUI) for users to configure account settings delegated to them by customer administrators.
- To Do – A productivity application that allows customers to manage, prioritize, and complete various tasks.
- Unified Feedback – A unified, global feedback system that is utilized by all Microsoft Purview, Microsoft Priva, and Microsoft Defender for Office solutions.
- Viva Glint – Improve engagement and performance with recommended actions and data-driven insights across employee lifecycle and organization-wide surveys.
- Viva Pulse – Empower managers to get feedback quickly and take action using brief team and project-based surveys in Microsoft Teams and on the web.
- Whiteboard Service – Brainstorm, plan, and share with others on a digital canvas, in real time. Whiteboard files are stored in SharePoint or OneDrive for Business.

M365 Microservices uses the following software to support the offerings listed above:

- 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 applications, with the exception of some service teams, which also leverage MyAccess through the Azure offering.
- Exchange Online (EXO) – Responsible for Microsoft's Outlook email service offering. Many Microsoft 365 services rely on Exchange's infrastructure and assets and follow the service's change management process.

M365 Microservices uses the following utilities to execute controls relevant to the M365 system:

- Employee Cloud Screening (ECS) – An SAP add-on 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, MyAccess, and Torus – M365 user management tools used to grant temporary user access time-bound permissions and access to sensitive systems, including access to customer content.
- Remote Desktop Services – The accepted method for Microsoft personnel to gain logical access to the M365 environment remotely using Remote Desktop Gateways (RDGs).
- Griffin/Office Supporting Infrastructure (OSI), M365SuiteUX Environments and Release Dashboard, PilotFish, and Azure DevOps – Change management tools used by service and support teams to track and deploy code changes to production environments.

- M365 OneBranch Release (MOBR) – An automated release solution available for internal use by M365 services.
- 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.

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 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, with the exception of some service teams, which utilize MyAccess 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 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 MyAccess.
- Azure – Provides customer authentication infrastructure including Microsoft Online Directory Services (MSODS), Microsoft Organization ID (OrgID), and 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	Content directly created by users. Content is not viewed by Microsoft personnel unless required to resolve a ticketed service problem.
End User Identifiable Information (EUII)	Data unique to a user or generated from a user's use of the service: • Linkable to an individual user • Does not contain customer content
Organization Identifiable Information (OII)	Data that can be used to identify a tenant (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	Administrator data Payment data Support data

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

Commitment to Competence

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

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

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

Compliance and Ethics — Board of Directors and Senior Leadership

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

Internal Audit Department

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

Audit Committee

The AC charter and responsibilities are on Microsoft's website, www.microsoft.com. The AC meets privately on a quarterly basis with Microsoft's external auditors and IA. The topics for the quarterly AC meetings are found in the AC Responsibilities Calendar set out in the charter. In addition, the AC influences the company through the IA function. The AC reviews the scope of IA and advises on the process of identifying and resolving issues. Lastly, the AC monitors itself by completing an annual self-evaluation.

Risk Assessment

Practices for identification of risk

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

Internal Audit — Fraud Risks

IA and the Financial Integrity Unit (FIU) look for fraud risk. The FIU performs procedures for the detection, investigation, and prevention of financial fraud affecting Microsoft worldwide. Fraud and abuse that is uncovered is reported to the Disclosure Committee. The FIU provides both a reactive and proactive response to allegations of fraud and abuse. The FIU uses a case management system that is also used by the Director of Compliance to

track cases and related metrics. The FIU interacts with Microsoft management, Corporate, External, and Legal Affairs (CELA), HR, Finance, Procurement, and others to determine specific fraud risks and responses.

Periodic Risk Assessment

IA and other groups within the company perform periodic risk assessments. 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 Microservices uses the following subservice organizations:

- Microsoft Azure including the Microsoft Datacenters service, which manages datacenters, IaaS, and PaaS supporting services for the M365 Microservices applications including hosting of servers, network support, authentication, virtual server hosting and system data storage as well as M365 which provides supporting services to the M365 Microservices.
- Microsoft 365 Central, which provides subscription-based access to a suite of online productivity applications and services for home and business use.

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

A brief overview of the subservice organizations used by M365 Microservices is below.

Organization	Brief Description
Microsoft Azure	Microsoft Azure's cloud PaaS offerings are used by M365 to host production data and handle logical access and change management controls for M365.
Microsoft Datacenters	Microsoft Datacenter's 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.
Microsoft M365 Central	M365 is used by M365 Microservices to host the Microservices on the existing M365 infrastructure.

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 service commitments and system requirements

or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements during the period October 1, 2022 to September 30, 2023.

Significant Changes

The Bookings Odata API service was deprecated and evidence was not retained for the auditor to test the C5 specific control listed in Section 4 of this report. However, there were no changes that are likely to affect report users' understanding of how the system is used to provide the Bookings Odata API service since the last issued report in 2022.

Description of Control Activities

This report leverages the TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, (AICPA, Trust Services Criteria). The description of control activities relevant to the trust criteria are included below. Additionally, the criteria for each principle and the relevant M365 Microservices controls in place to satisfy the criteria are included as a separate matrix and are an integral part of the description of the system.

Business Planning

The M365 planning process is driven by product updates and releases. Senior management defines the vision and strategy for the overall M365 product on an annual basis. During this process, senior management considers its high-level commitments and requirements to security, availability, processing integrity, and confidentiality in a series of planning meetings and communicates the output to M365 personnel through a strategy memo. The M365 Development and Project Management team leads also consider their teams' commitments to security, availability, processing integrity, and confidentiality on a more specific level and communicate the outcome in component planning meetings. These commitments are then converted into design considerations for implementation during the product releases. Implementation of these requirements is advised by the M365 Security team, which is responsible for overseeing security issues, system operation, and service availability within the M365 environment. In addition, an M365 GRC risk team has been defined and is responsible for management of security, availability, processing integrity, and confidentiality controls within the M365 environment. Finally, service teams have personnel who are responsible for system operation, service availability, and control implementation. Each team works to implement and maintain the commitments for security, availability, processing integrity, and confidentiality.

Hiring Process

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 use it to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and to make an appropriate hiring decision.

Performance Review

Microsoft employees create individual accountabilities that align with those established for their manager, organization, and Microsoft. Each accountability is supported with customer-centric actions and measures so that M365 personnel are working toward the same overarching vision. Accountabilities are established when an employee is hired and then updated throughout the year according to business needs.

Periodically, performance reviews, called "Connects", are held between employees and their managers, during which progress is analyzed against accountabilities and accountabilities are adjusted, if needed. The manager evaluates the individual's contributions to the team and business or customer impact, taking into consideration

contributions towards creating a high performing team and the demonstration of competencies relevant to their role.

Standards of Business Conduct

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

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 ECS.

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 ECS. Background check information for FTEs and Vendors is pushed from ECS 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.

Workload 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.

System Description

Information regarding the design and operation of M365, including Service Level Agreements (SLAs), is available to customers on the Internet in many locations, including www.microsoft.com. Additional system description details are available for customers and potential customers through third-party audit and attestation reports as well as control documentation through the Service Trust Portal in the Admin Portal. A specific view of the M365 environment is used internally to analyze key processes for system operation.

Customer Commitments and Responsibilities

Externally, M365 communicates its commitments, including those related to regulations, security, availability, processing integrity, and confidentiality to customers through contracts and SLAs. Internally, these commitments are reflected in a control framework, which is refreshed on an annual basis with control owners. These commitments and the associated control framework are distributed to M365 employees through policies, training, and Office Hours. Office Hours are twice-weekly time slots set aside during which M365 teams may

speak with the GRC team to discuss topics including security, availability, and regulatory information, and how that information could impact their relevant areas of the control framework.

In addition to communicating commitments to its customers, M365 communicates the responsibilities of the customer to use the services. These responsibilities are described in SLAs, contracts, audit and attestation reports issued by independent auditors, and through descriptions available on Microsoft websites.

Policies

All Microsoft M365 staff and contingent staff are accountable for understanding and adhering to the guidance contained in the Microsoft Security Policy and applicable supporting standards. Individuals not employed by Microsoft but allowed to access, manage, or process information assets of Microsoft are also accountable for understanding and adhering to the guidance contained in the Security Policy and Standards. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification, risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the Microsoft intranet.

Security and Availability Incident Communication

M365 has established incident response procedures and centralized tracking tools, which consist of different channels for reporting production system incidents and weaknesses. Security and availability monitoring tools include Aria, Geneva, Incident Manager (IcM), Jarvis, Vanquish, and Office Substrate Pulse. Incidents may also be reported via email by different M365 teams or Microsoft groups, such as the specific application and supporting services teams, Azure teams, or Microsoft Datacenters teams. The security teams operate 24x7x365 event/incident monitoring and response services. External users may communicate security and availability incidents to Microsoft and receive updates through Customer Support, the online customer portal, or the customer service number.

Service Infrastructure and Support Systems Change Management Communication

Customers may view prior or upcoming upgrades and changes to the M365 service infrastructure in the Microsoft M365 blog. In addition, M365 customers receive notifications of major changes prior to change implementation through the customer portal. See the section “Service infrastructure and support systems change management” below for a description of the overall infrastructure and application change management process.

Risk Assessment – M365

M365 performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and the risk from these threats is formally assessed. The information gained from the assessment is used to create and prioritize work items.

M365 is represented on the Operational Enterprise Risk Management (OERM) Governance Committee by the M365 Risk Management Office. For M365 the risk review is done annually, beginning in August. M365 risk management contacts the M365 GRC Working Group directly for updates to the overall environment and discussion of risk issues identified during the assessment process. The result of these procedures is a report sent to the corporate Vice President of the Office Product Group for review and approval. M365 risk management also sends information to the OERM for inclusion in the annual report that is sent to the Microsoft Board of Directors in December.

Control Design and Implementation

Based on the risk assessment performed, control activities are put in place within the M365 control framework. This framework is managed by the M365 GRC group and is evaluated and updated on an ongoing basis. This

evaluation includes input from changes to the overall M365 environment, the regulatory landscape, and results of control assessments.

Implementation of the control activities is the responsibility of each of the M365 application and supporting service teams.

Data Flow Diagrams

Data flow diagrams showing M365 system interactions and dependencies are maintained for each service. On an annual basis, these diagrams are updated by GRC personnel with the input of relevant service teams. This is done to provide up to date M365 system design information to M365 personnel to provide them with an understanding of their role in the system and additional background for addressing system security, availability, processing integrity, and confidentiality-related issues.

Control Monitoring

The design and implementation of security, availability, processing integrity, and confidentiality controls are analyzed by a third party at least once per year. These assessments include external (e.g., ISO and FedRAMP audits) and internal evaluations (e.g., risk assessments and vulnerability scans). The results and findings from these assessments are addressed with corrective actions, which are tracked by the M365 GRC team to substantiate that they are addressed in a timely manner.

Access Management

All access to customer content is governed by the IDM service and follows the Just-in-Time access described within this report. Service teams may use other identity access management tools to manage access to internal tools and systems that don't store customer content.

Identity Access Management

Microsoft M365 owns and manages tools that regulate access to M365 production environments. Most service teams use the IDM access management service to limit access to authorized users. The service, managed by the Access Control team, allows each of the other service teams to manage their respective servers 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 MyAccess. Additionally, for Microsoft 365 OneBranch Release (MOBR), access is regulated by Azure.

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, workloads have security groups that have a set expiration period from when an account was granted access to the group.

For manually maintained user access, a manual user access review is performed on a periodic basis to substantiate that access for each user is relevant and in line with job responsibilities. Any needed access alterations identified during the review are addressed in a timely manner.

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 Windows AD 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.

Mobile Devices

For Microsoft employees and other internal users, access to M365 applications and supporting services infrastructure through mobile devices is restricted and managed by the Microsoft Datacenters group.

External users – External users will go through the same authentication process to access M365 applications regardless of device. The external users' access is managed and configured by the customer.

Data Management

Data Transmission (Encryption)

Encryption between Microsoft employee and datacenter connection

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

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

Encryption between client and Microsoft datacenter connection

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

Encryption between Microsoft datacenters

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

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:

- Automated build-out tool:

  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.

Antimalware

Through the server build-out process, each application and supporting service has an antimalware agent installed. The antimalware agent is configured to obtain the latest available definition files on a master antimalware server. If there are issues related to the agent synchronization process with the master server, the individual server's antimalware agent automatically notifies the SIR team, and the reported issue is analyzed and resolved.

Data at Rest (Encryption)

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

Data Segregation

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

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.

Availability Monitoring

M365 applications and supporting services utilize different tools to monitor and evaluate their service's health (i.e., capacity, resiliency, and availability). These tools are configured to automatically alert assigned team members of issues impacting service health. For each service team, there are 24x7 On-Call Engineers, or "OCEs", that monitor and resolve the issues that are reported or identified. Each service utilizes their own custom tools to monitor their respective service's health. These tools are described in the *Software* section of the report above.

In addition to the above monitoring, M365 senior management reviews capacity, availability, and resiliency reports from the above tools, for anomalies and deviations that could impact availability. On a monthly basis,

M365 teams prepare an overview of the service team's capacity, availability, and resiliency from the prior month. This overview presents the root cause of anomalies or deviations to senior management and based on the meeting issues or changes to capacity and availability are tracked to resolution.

Data Replication and Data Backup

The M365 Microservices teams defined in this report use Azure for data replication and data backup services. Where applicable, Azure performs replication and backup of customer content.

Business Continuity

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

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.

Processing and Data Integrity

M365 processes data uploaded and managed by the customers per agreed upon processes and procedures. As part of the geographic replication process, data being replicated between datacenters is monitored for completeness and accuracy.

Confidentiality

M365 monitors its dependencies on third parties through obtaining and evaluating attestation reports when available.

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.

M365 will remove customer content per contract agreements based on customer account status (e.g., Terminated, Suspended).

Trust Criteria and Related Control Activities

Trust criteria mapped to the related control activities is documented below under "Trust Services Criteria and Control Activities provided by Microsoft." The testing procedures performed over the related control activities are listed below. 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.

Principal Service Commitments and System Requirements

Microsoft makes service commitments to its customers and has established system requirements as part of the M365 service. Some of these commitments are principal to the performance of the service and relate to

applicable trust services criteria. M365 is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that M365's service commitments and system requirements are achieved.

Service commitments to customers are documented and communicated in Service Level Agreements (SLAs) and other customer agreements such as the Microsoft Product Terms (formerly called Online Service Terms), Data Protection Addendum (DPA), Microsoft Privacy Statement, and Microsoft Trust Center, as well as in the description of the service offering provided online. Service commitments include, but are not limited to, the following:

- Security: M365 has made commitments related to securing customer data and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, physical security and other relevant security controls.
- Availability: M365 has made commitments related to percentage uptime and connectivity for Azure as well as commitments related to service credits for instances of downtime.
- Processing Integrity: M365 has made commitments related to processing customer actions completely, accurately and timely. These customer actions include, for example, specifying geographic regions for the storage and processing of customer data.
- Confidentiality: M365 has made commitments related to maintaining the confidentiality of customers' data through data classification policies, data encryption and other relevant security controls.

Microsoft has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements including the following:

- Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained.
- In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of various M365 services and offerings.
- Procedures are in place so that the access, collection, use, and deletion of customer data is in accordance with the service commitments.
- Policies and instructions for controlling and monitoring third parties (e.g. service providers or suppliers) whose services contribute to the provision of the cloud service are documented and communicated.
- M365 services are designed to maintain high availability through redundancy and replication.
- Critical systems are monitored through third-party and internal tools to maintain availability.
- Access to physical and logical assets is limited to authorized users and is provisioned based on job requirements to mitigate risk of unauthorized access.
- Incidents impacting internal and customer systems are detected, escalated and resolved.
- Development of new features and major changes to M365 services are performed in accordance with policies and procedures.
- Once Microsoft becomes aware of a breach of security that would impact Customers, Professional services or personal data; Microsoft will (1) notify Impacted Customers of the security incident, (2) Investigate the

Security Incident and provide the details to the impacted customer, (3) take reasonable steps to mitigate the incident.

Such requirements are communicated in M365's system policies and procedures, system design documentation, and contracts with customers. Microsoft's service commitments and system requirements are designed based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality, and other frameworks.

Complementary User Entity Control Considerations

Microsoft M365 Microservices 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 Microservices. The following list contains controls that M365 Microservices 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 SOC 2 Control Criteria
CUEC-01: User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access.	CC6.1, CC6.2, CC6.3, CC6.6
CUEC-02: User entities establish proper controls over the use of system IDs and passwords.	CC6.6
CUEC-03: User entities are responsible for managing their user's password authentication mechanism.	CC6.6
CUEC-04: User entities enforce desired level of encryption for network sessions.	CC6.1, CC6.7, C1.1
CUEC-06: User entities secure the software and hardware used to access M365.	CC6.1, CC6.3, CC6.6, CC6.7, CC6.8, CC7.1, A1.2
CUEC-07: User entities conduct end-user training.	CC7.2, CC9.2
CUEC-08: User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.	CC3.2, CC7.2, CC7.3, CC7.4, CC7.5, CC9.2, PI1.1
CUEC-10: User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality.	CC2.3, CC6.5, CC6.7, CC7.5, PI1.1, PI1.5
CUEC-11: User entities are responsible for managing their data inputs, and data uploads to M365 for completeness, accuracy, and timeliness.	PI1.2
CUEC-12: User entities are responsible for managing their data processing within M365 for completeness, accuracy, and timeliness.	PI1.1, PI1.2, PI1.3
CUEC-13: User entities are responsible for managing their stored data for completeness and accuracy.	PI1.5

Complementary User Entity Controls	Relevant SOC 2 Control Criteria
CUEC-14: User entities are responsible for managing their data output from M365 for completeness, accuracy, and timeliness.	PI1.4

Complementary Subservice Organization Controls

Microsoft's controls related to the M365 Microservices system detailed in this report cover only a portion of overall internal control for each user entity of M365 Microservices. It is not feasible for the related control criteria related to M365 Microservices to be achieved solely by Microsoft. Therefore, in conjunction with M365 Microservices' controls, a user entity must take into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as follows. Note that the CSOCs associated with the subservice organizations are summarized in the table below, refer to control mapping for more on the specific CSOC associated with the criteria.

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant SOC 2 Control Criteria
Platform as a Service/Infrastructure as a Service	Microsoft Azure	Microsoft Azure is responsible for maintaining controls over access management (including authentication), change management, operational controls, and data protection to the platform services supporting M365. Additionally, for services using Azure, Azure is responsible for maintaining controls over: • secure transmission, handling, and storage of data (including encryption, backups, replication, and recovery). • security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management for M365 services hosted on the Azure platform.	CC6.1, CC6.2, CC6.3, CC6.5, CC6.6, CC6.7, CC7.1, CC7.2, CC7.3, CC7.4, CC7.5, CC9.1, A1.2, A1.3, C1.1, PI1.5

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant SOC 2 Control Criteria
Infrastructure as a Service	Microsoft Datacenters	Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities supporting M365, including datacenters. Additionally, Microsoft Datacenters is responsible for maintaining controls over: • protection of the network environment, including perimeter firewalls, restricting access to network devices and monitoring network devices for compliance with security standards. • physical access to the facilities, including data centers, supporting M365. • environmental threats (including natural disasters and man-made threats). • physical data storage, protection, and disposal services supporting M365.	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC6.8, CC7.1, CC7.2, CC7.3, CC7.4, CC7.5, CC9.1, A1.2, A1.3, C1.1, PI1.5
Authentication, Logical Access, Security and Incident Management, Vulnerability Scanning, Patch Management	Microsoft 365 Central	Microsoft 365 Central service is responsible for maintaining controls over authentication and logical access. Additionally, Microsoft 365 Central service is responsible for maintaining controls over the security and incident management, vulnerability scanning and patch management.	CC6.1, CC6.2, CC6.3, CC.6.6, CC6.7, CC6.8, CC7.1, CC7.2, CC7.3, CC7.4, CC7.5

Trust Services Criteria and M365 Microservices Control Activities provided by Microsoft

Note: There are certain gaps in control activity numbering as a result of updates to the control environment and supporting policies and procedures. Thus, the following control numbers are intentionally omitted: CA-26, CA-27, CA-28, CA-39, CA-40, CA-41, CA-42, CA-47, CA-48, CA-52, CA-56 to CA-65, ELC-05, ELC-13, and ELC-14.

Criteria Common to All Security, Availability, Processing Integrity, and Confidentiality Principles

CC1.0 – Common Criteria Related to Control Environment

Criteria	Microsoft 365 Control Activity
CC1.1 – COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	**CA-04 –** Employees hold periodic "connects" with their managers to validate they are on the expected Career Path and facilitate greater collaboration. They also review their performance against their documented deliverables (priorities) and discuss the results with their managers. **CA-07 –** Microsoft Compliance & Ethics team updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Compliance & Ethics team provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately. **CA-17 –** Microsoft 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) compromised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet. **ELC-01** – Microsoft's values are accessible to employees via the Values SharePoint site and are updated as necessary by management. **ELC-02 –** Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct. **ELC-08 –** Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, including the consequences of violating relevant laws, regulations, provisions, and policies regarding information security. Employees are required to acknowledge agreements to return Microsoft assets upon termination.

Criteria	Microsoft 365 Control Activity
CC1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	**CA-17 –** Microsoft 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) compromised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet. **ELC-03 –** The Audit Committee (AC) reviews its Charter and Responsibilities as listed in its calendar on an annual basis. The AC Responsibilities include meeting with the external and internal auditors on a quarterly basis; providing oversight on the development and performance of controls; and completing an annual self-evaluation. **ELC-04 –** Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.
CC1.3 – COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	**CA-01 –** A Microsoft 365 security team has been defined and is responsible for Security issues within the Microsoft 365 environment. Service teams have operations personnel who are responsible for system operation and service availability. **CA-02 –** A Microsoft 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, availability, confidentiality, and processing integrity controls within the Microsoft 365 environment. **CA-17 –** Microsoft 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) compromised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet. **ELC-04 –** Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.

Criteria	Microsoft 365 Control Activity
CC1.4 – COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CA-04 – Employees hold periodic "connects" with their managers to validate they are on the expected Career Path and facilitate greater collaboration. They also review their performance against their documented deliverables (priorities) and discuss the results with their managers. CA-06 – The Candidates job descriptions are created and documented for open positions within M365. Job descriptions include desired candidate competencies and expected job roles and responsibilities. CA-07 – Microsoft Compliance & Ethics team updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Compliance & Ethics team provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately. CA-08 – The Microsoft 365 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 Microsoft 365 production assets containing customer content. CA-17 – Microsoft 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) compromised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet. ELC-01 – Microsoft's values are accessible to employees via the Values SharePoint site and are updated as necessary by management. ELC-06 – The Compensation Committee is responsible for reviewing and discussing plans for executive officer development and corporate succession plans for the CEO and other executive officers.

Criteria	Microsoft 365 Control Activity
CC1.5 – COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CA-01 – A Microsoft 365 security team has been defined and is responsible for Security issues within the Microsoft 365 environment. Service teams have operations personnel who are responsible for system operation and service availability. CA-04 – Employees hold periodic "connects" with their managers to validate they are on the expected Career Path and facilitate greater collaboration. They also review their performance against their documented deliverables (priorities) and discuss the results with their managers. CA-06 – The Candidates job descriptions are created and documented for open positions within M365. Job descriptions include desired candidate competencies and expected job roles and responsibilities. CA-07 – Microsoft Compliance & Ethics team updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Compliance & Ethics team provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately. CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing M365 and prioritize the most preeminent risks based on impact, likelihood, and management's controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by M365 management with ownership assigned out to individual teams and their management. ELC-02 – Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct. ELC-08 – Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, including the consequences of violating relevant laws, regulations, provisions, and policies regarding information security. Employees are required to acknowledge agreements to return Microsoft assets upon termination. ELC-12 – Management expects outsourced providers to meet certain levels of skills and experience, depending on the role and holds them accountable to achieving specific deliverables, as outlined in a Statement of Work. Outsourced providers are trained to understand and comply with Microsoft's supplier code of conduct.

CC2.0 – Common Criteria Related to Communication and Information

Criteria	Microsoft 365 Control Activity
CC2.1 – COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CA-02 – A Microsoft 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, availability, confidentiality, and processing integrity controls within the Microsoft 365 environment. CA-03 – Senior Management, as part of its major system release planning process, considers its commitments and requirements for Security, availability, confidentiality, and processing integrity. CA-05 – The Governance, Risk, and Compliance team updates the data flow diagrams and service offerings of M365 with the individuals that act as point of contact for each service offering. CA-11 – On an annual basis services are updated to reflect changes made to the Microsoft 365 control framework. CA-17 – Microsoft 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) compromised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet. CA-25 – Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Microsoft 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes. ELC-04 – Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment. ELC-07 – The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.

Criteria	Microsoft 365 Control Activity
CC2.2 – COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	**CA-02 –** A Microsoft 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, availability, confidentiality, and processing integrity controls within the Microsoft 365 environment **CA-07 –** Microsoft Compliance & Ethics team updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Compliance & Ethics team provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately. **CA-11 –** On an annual basis services are updated to reflect changes made to the Microsoft 365 control framework. **CA-12 –** Microsoft 365 communicates its commitments to customers in SLAs. These commitments are reflected in the control framework, which defines regulatory, security, availability, confidentiality, and processing integrity requirements. This information is distributed internally through policies, training, and Office Hours. **CA-16 –** Customers can report issues and potential incidents by creating a service request through the admin portal, which includes the option for telephone support. Service request status and activity can be viewed through the Admin Center. **CA-24 –** Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner. **CA-25 –** Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Microsoft 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes. **C5-CA-01 –** Microsoft has policies documented to cover the development of information systems within the Microsoft 365 environment. Policies are communicated to M365 service teams and cover the following: - Security standards - Security Development Lifecycle - Version control - Programming policies

Criteria	Microsoft 365 Control Activity
CC2.2 – COSO Principle 14 (continued): The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	**C5-CA-03 –** Microsoft has policies documented to cover the management and provisioning of system and data access for the Microsoft 365 environment. Policies are communicated to M365 service teams and cover the following: - Provisioning of access - Separation of duties - Role/Eligibility approval process - Access termination - Required access control documentation **C5-CA-08** – Microsoft has policies and instructions documented to cover protection for data in motion, based on risk. Policies are communicated to M365 service teams. **C5-CA-09 –** Microsoft has policies and instructions documented to cover encryption procedures and key management within the Microsoft 365 environment. Policies are communicated to M365 service teams. **ELC-02 –** Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct. **ELC-08 –** Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, including the consequences of violating relevant laws, regulations, provisions, and policies regarding information security. Employees are required to acknowledge agreements to return Microsoft assets upon termination.

Criteria	Microsoft 365 Control Activity
CC2.3 – COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	CA-07 – Microsoft Compliance & Ethics team updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Compliance & Ethics team provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately. CA-10 – Microsoft 365 provides customers and external users self-service compliance reporting related to Microsoft 365's services and systems within the Service Trust Portal website. In addition to compliance reporting, the Service Trust Portal details the customer's and external user's responsibilities for service and system operation. CA-12 – Microsoft 365 communicates its commitments to customers in SLAs. These commitments are reflected in the control framework, which defines regulatory, security, availability, confidentiality, and processing integrity requirements. This information is distributed internally through policies, training, and Office Hours. CA-14 – Changes and updates to the Microsoft 365 environment are communicated through the Message Center which is part of the Microsoft 365 Admin Center. CA-15 – Service impacting incidents, including security incidents, are communicated to the customer through the Service Health Center. CA-16 – Customers can report issues and potential incidents by creating a service request through the admin portal, which includes the option for telephone support. Service request status and activity can be viewed through the Admin Center. CA-53 – Microsoft 365 monitors its dependencies on third parties through obtaining and evaluating attestation reports when available. ELC-02 – Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct. ELC-08 – Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, including the consequences of violating relevant laws, regulations, provisions, and policies regarding information security. Employees are required to acknowledge agreements to return Microsoft assets upon termination. *Complementary User Entity Controls* CUEC-10 – User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality.

CC3.0 – Common Criteria Related to Risk Assessment

Criteria	Microsoft 365 Control Activity
CC3.1 – COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**CA-01 –** A Microsoft 365 security team has been defined and is responsible for Security issues within the Microsoft 365 environment. Service teams have operations personnel who are responsible for system operation and service availability. **CA-02 –** A Microsoft 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, availability, confidentiality, and processing integrity controls within the Microsoft 365 environment. **CA-03 –** Senior Management, as part of its major system release planning process, considers its commitments and requirements for Security, availability, confidentiality, and processing integrity. **CA-09 –** Microsoft 365 system information regarding the design and operation of its services is available to users online through Microsoft web portal. **CA-22 –** Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing M365 and prioritize the most preeminent risks based on impact, likelihood, and management's controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by M365 management with ownership assigned out to individual teams and their management. **CA-23 –** Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis. **CA-24 –** Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner. **CA-25 –** Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Microsoft 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes. **C5-CA-17 –** Microsoft 365 performs an annual Information Security Management System (ISMS) review and reviews results with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. **C5-CA-18 –** Microsoft 365 has a defined exception program where exceptions are reviewed and tracked. The results of the review process are documented, and if approved the exception is limited in time and reviewed at least annually by relevant risk owners. **C5-CA-21 –** Prior to contracting with Microsoft, suppliers undergo a risk assessment based on the services that will be provided and data handled. List of reviewed suppliers is maintained and their risk profiles are reviewed at least annually.

Criteria	Microsoft 365 Control Activity
CC3.1 – COSO Principle 6 (continued): The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**ELC-04 –** Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment. **ELC-07 –** The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **ELC-12 –** Management expects outsourced providers to meet certain levels of skills and experience, depending on the role and holds them accountable to achieving specific deliverables, as outlined in a Statement of Work. Outsourced providers are trained to understand and comply with Microsoft's supplier code of conduct. **ELC-15 –** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Microsoft 365 environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.
CC3.2 – COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	**CA-13 –** Incident response guides are used by Microsoft 365 personnel for the handling and reporting of security incidents. These guides are stored on internal SharePoint sites and are updated as needed. **CA-17 –** Microsoft 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) compromised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet. **CA-22 –** Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing M365 and prioritize the most preeminent risks based on impact, likelihood, and management's controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by M365 management with ownership assigned out to individual teams and their management. **CA-23 –** Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis. **CA-24 –** Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner.

Criteria	Microsoft 365 Control Activity
CC3.2 – COSO Principle 7 (continued): The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	**CA-25 –** Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Microsoft 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes. **CA-53 –** Microsoft 365 monitors its dependencies on third parties through obtaining and evaluating attestation reports when available. **C5-CA-17 –** Microsoft 365 performs an annual Information Security Management System (ISMS) review and reviews results with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. **C5-CA-18 –** Microsoft 365 has a defined exception program where exceptions are reviewed and tracked. The results of the review process are documented, and if approved the exception is limited in time and reviewed at least annually by relevant risk owners. **ELC-04 –** Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment. **ELC-07 –** The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **ELC-09** – Microsoft's Enterprise Business Continuity program is intended to ensure that Microsoft is ready to mitigate risks and vulnerabilities and respond to a major disruptive event in a manner that enables the business to continue to operate in a safe, predictable, and reliable way. The EBCM charter provides a strategic direction and leadership to all Microsoft Engineering organizations. EBCM is governed through the Program Management Office to ensure that the program adheres to a coherent long-term vision and mission, and is consistent with enterprise program standards, methods, policies, and metrics. *Complementary User Entity Controls* **CUEC-08 –** User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.

Criteria	Microsoft 365 Control Activity
CC3.3 – COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CA-17 – Microsoft 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) compromised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet. CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing M365 and prioritize the most preeminent risks based on impact, likelihood, and management's controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by M365 management with ownership assigned out to individual teams and their management. CA-23 – Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis. CA-24 – Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner. CA-25 – Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Microsoft 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes. CA-53 – Microsoft 365 monitors its dependencies on third parties through obtaining and evaluating attestation reports when available. ELC-07 – The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.

Criteria	Microsoft 365 Control Activity
CC3.4 – COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	**CA-22 –** Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing M365 and prioritize the most preeminent risks based on impact, likelihood, and management's controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by M365 management with ownership assigned out to individual teams and their management. **CA-23 –** Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis. **CA-24 –** Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner. **CA-25 –** Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Microsoft 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes. **CA-53 –** Microsoft 365 monitors its dependencies on third parties through obtaining and evaluating attestation reports when available. **ELC-04 –** Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment. **ELC-06 –** The Compensation Committee is responsible for reviewing and discussing plans for executive officer development and corporate succession plans for the CEO and other executive officers. **ELC-07 –** The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.

CC4.0 – Common Criteria Related to Monitoring Activities

Criteria	Microsoft 365 Control Activity
CC4.1 – COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	**CA-02 –** A Microsoft 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, availability, confidentiality, and processing integrity controls within the Microsoft 365 environment. **CA-05 –** The Governance, Risk, and Compliance team updates the data flow diagrams and service offerings of M365 with the individuals that act as point of contact for each service offering. **CA-22 –** Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing M365 and prioritize the most preeminent risks based on impact, likelihood, and management's controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by M365 management with ownership assigned out to individual teams and their management. **CA-24 –** Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner. **CA-25 –** Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Microsoft 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes. **ELC-04 –** Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment. **ELC-07 –** The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **ELC-11 –** Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. Audit findings are addressed relative to their criticality.

Criteria	Microsoft 365 Control Activity
CC4.2 – COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	**CA-05 –** The Governance, Risk, and Compliance team updates the data flow diagrams and service offerings of M365 with the individuals that act as point of contact for each service offering. **CA-11 –** On an annual basis services are updated to reflect changes made to the Microsoft 365 control framework. **CA-15** – Service impacting incidents, including security incidents, are communicated to the customer through the Service Health Center. **CA-24** – Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner. **ELC-04** – Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment. **ELC-11 –** Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. Audit findings are addressed relative to their criticality.

CC5.0 – Common Criteria Related to Control Activities

Criteria	Microsoft 365 Control Activity
CC5.1 – COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	**CA-02 –** A Microsoft 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, availability, confidentiality, and processing integrity controls within the Microsoft 365 environment. **CA-11 –** On an annual basis services are updated to reflect changes made to the Microsoft 365 control framework. **CA-17 –** Microsoft 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) compromised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet. **CA-22 –** Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing M365 and prioritize the most preeminent risks based on impact, likelihood, and management's controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by M365 management with ownership assigned out to individual teams and their management. **CA-23 –** Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis. **CA-25 –** Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Microsoft 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes. **ELC-07 –** The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **ELC-10 –** Teams evaluate changes according to criteria defined by GRC. Changes that meet the criteria go through a review that includes a risk assessment.

Criteria	Microsoft 365 Control Activity
CC5.2 – COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	**CA-02 –** A Microsoft 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, availability, confidentiality, and processing integrity controls within the Microsoft 365 environment. **CA-11 –** On an annual basis services are updated to reflect changes made to the Microsoft 365 control framework. **CA-17 –** Microsoft 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) compromised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet. **CA-22 –** Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing M365 and prioritize the most preeminent risks based on impact, likelihood, and management's controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by M365 management with ownership assigned out to individual teams and their management. **CA-23 –** Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis. **CA-25 –** Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Microsoft 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes. **ELC-07 –** The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **ELC-10 –** Teams evaluate changes according to criteria defined by GRC. Changes that meet the criteria go through a review that includes a risk assessment.

Criteria	Microsoft 365 Control Activity
CC5.3 – COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	**CA-02 –** A Microsoft 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, availability, confidentiality, and processing integrity controls within the Microsoft 365 environment. **CA-07 –** Microsoft Compliance & Ethics team updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Compliance & Ethics team provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately. **CA-11 –** On an annual basis services are updated to reflect changes made to the Microsoft 365 control framework. **CA-17 –** Microsoft 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) compromised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet. **CA-22 –** Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing M365 and prioritize the most preeminent risks based on impact, likelihood, and management's controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by M365 management with ownership assigned out to individual teams and their management. **CA-23 –** Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis. **CA-25 –** Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Microsoft 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes. **C5-CA-01 –** Microsoft has policies documented to cover the development of information systems within the Microsoft 365 environment. Policies are communicated to M365 service teams and cover the following: - Security standards - Security Development Lifecycle - Version control - Programming policies

Criteria	Microsoft 365 Control Activity
CC5.3 – COSO Principle 12 (continued): The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	**C5-CA-03 –** Microsoft has policies documented to cover the management and provisioning of system and data access for the Microsoft 365 environment. Policies are communicated to M365 service teams and cover the following: - Provisioning of access - Separation of duties - Role/Eligibility approval process - Access termination - Required access control documentation **C5-CA-07** – Cryptographic controls are used for information protection within the Microsoft 365 service based on the Microsoft 365 Cryptographic Policy and Key Management procedures. **C5-CA-08 –** Microsoft has policies and instructions documented to cover protection for data in motion, based on risk. Policies are communicated to M365 service teams. **C5-CA-09 –** Microsoft has policies and instructions documented to cover encryption procedures and key management within the Microsoft 365 environment. Policies are communicated to M365 service teams. **C5-CA-13 –** (1) Microsoft has policies and instructions documented to communicate the secure collection and storage of metadata within the Microsoft 365 environment. Policies are communicated to M365 service teams. (2) Metadata is collected and used in accordance with contractual commitments. **ELC-04 –** Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.

CC6.0 – Common Criteria Related to Logical and Physical Access Controls

Criteria	Microsoft 365 Control Activity
CC6.1 – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CA-08 – The Microsoft 365 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 Microsoft 365 production assets containing customer content. CA-32 – Access to shared accounts within the Microsoft 365 environment are restricted to authorized personnel. CA-33.a – 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. CA-33.b – Elevated access within the M365 production environment is approved by an authorized user. CA-34 – Identity of users is authenticated to Microsoft 365 Services. The use of passwords incorporates policy on periodic change and password complexity. CA-35.a – Access to privileged accounts is configured to be revoked automatically based on access expiration settings, including inactivity and Manager / Cost Center changes. CA-35.b[4] – Elevated access within the M365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis. CA-36 – Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment. CA-37 – Each Microsoft 365 Service Customer's content is segregated from other Online Services customers' content to isolate customer tenant data flows. C5-CA-01 – Microsoft has policies documented to cover the development of information systems within the Microsoft 365 environment. Policies are communicated to M365 service teams and cover the following: - Security standards - Security Development Lifecycle - Version control - Programming policies

[4] An exception was identified for this control related to Productivity Applications and Services and Bing Teams. Productivity Applications and Services - One relevant group was not included in the User Access Review for the sampled quarter from for the Tasks – Business Scenario Service. Bing Teams - No exceptions noted during Deloitte & Touche LLP's testing. However, Internal Audit (IA) noted that for the Microsoft Search in Bing (MSB) team, 2 of 8 security groups with privileged repository access were not reviewed. The access was not reviewed. The access for all users within the security groups was deemed appropriate.

Criteria	Microsoft 365 Control Activity
CC6.1 (continued) – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	C5-CA-03 – Microsoft has policies documented to cover the management and provisioning of system and data access for the Microsoft 365 environment. Policies are communicated to M365 service teams and cover the following: - Provisioning of access - Separation of duties - Role/Eligibility approval process - Access termination - Required access control documentation C5-CA-04[5] – Cryptographic certificates, keys, and customer access keys used for communication between Azure and Microsoft 365 services and other internal components are stored securely. C5-CA-05 – Code repositories are used for managing source code changes to the Microsoft 365 platform. Procedures are established for authorized M365 personnel to submit source code changes. Authorization is based on role. C5-CA-06 – Network traffic within the Microsoft 365 environment is segregated to separate customer traffic from management traffic. C5-CA-07 – Cryptographic controls are used for information protection within the Microsoft 365 service based on the Microsoft 365 Cryptographic Policy and Key Management procedures. C5-CA-10 – M365 has established policies for mobile computing devices to meet appropriate security practices prior to being connected to the production environment. C5-CA-15 – The access and management of the logging and monitoring functionalities is limited to select personnel. Changes to the logging and monitoring are approved by the engineering teams. *Complementary Subservice Organization Controls* CSOC – 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. CSOC – 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. CSOC – Microsoft 365 Central – Microsoft 365 Central service is responsible for maintaining controls over authentication and logical access.

[5] An exception was identified for this control related to Bookings Odata API. Bookings Odata API - Per inquiry with management, noted that the company did not retain evidence for testing of this control.

Criteria	Microsoft 365 Control Activity
CC6.1 (continued) – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	*Complementary User Entity Controls* **CUEC-01 –** User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access. **CUEC-04 –** User entities enforce desired level of encryption for network sessions. **CUEC-06 –** User entities secure the software and hardware used to access M365.

Criteria	Microsoft 365 Control Activity
CC6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	CA-08 – The Microsoft 365 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 Microsoft 365 production assets containing customer content. CA-33.a – 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. CA-33.b – Elevated access within the M365 production environment is approved by an authorized user. CA-35.a – Access to privileged accounts is configured to be revoked automatically based on access expiration settings, including inactivity and Manager / Cost Center changes. CA-35.b[4] – Elevated access within the M365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis. CA-43 – When users no longer require access or upon termination the user access privileges are revoked in a timely manner. C5-CA-03 – Microsoft has policies documented to cover the management and provisioning of system and data access for the Microsoft 365 environment. Policies are communicated to M365 service teams and cover the following: - Provisioning of access - Separation of duties - Role/Eligibility approval process - Access termination - Required access control documentation C5-CA-04[5] – Cryptographic certificates, keys, and customer access keys used for communication between Azure and Microsoft 365 services and other internal components are stored securely. C5-CA-05 – Code repositories are used for managing source code changes to the Microsoft 365 platform. Procedures are established for authorized M365 personnel to submit source code changes. Authorization is based on role. C5-CA-07 – Cryptographic controls are used for information protection within the Microsoft 365 service based on the Microsoft 365 Cryptographic Policy and Key Management procedures. C5-CA-10 – M365 has established policies for mobile computing devices to meet appropriate security practices prior to being connected to the production environment.

Criteria	Microsoft 365 Control Activity
CC6.2 (continued) – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	*Complementary Subservice Organization Controls* **CSOC – 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. **CSOC – 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. **CSOC – Microsoft 365 Central –** Microsoft 365 Central service is responsible for maintaining controls over authentication and logical access. *Complementary User Entity Controls* **CUEC-01 –** User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access.

Criteria	Microsoft 365 Control Activity
CC6.3 – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	CA-08 – The Microsoft 365 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 Microsoft 365 production assets containing customer content. CA-33.a – 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. CA-33.b – Elevated access within the M365 production environment is approved by an authorized user. CA-35.a – Access to privileged accounts is configured to be revoked automatically based on access expiration settings, including inactivity and Manager / Cost Center changes. CA-35.b[4] – Elevated access within the M365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis. CA-43 – When users no longer require access or upon termination the user access privileges are revoked in a timely manner. C5-CA-03 – Microsoft has policies documented to cover the management and provisioning of system and data access for the Microsoft 365 environment. Policies are communicated to M365 service teams and cover the following: - Provisioning of access - Separation of duties - Role/Eligibility approval process - Access termination - Required access control documentation C5-CA-04[5] – Cryptographic certificates, keys, and customer access keys used for communication between Azure and Microsoft 365 services and other internal components are stored securely. C5-CA-05 – Code repositories are used for managing source code changes to the Microsoft 365 platform. Procedures are established for authorized M365 personnel to submit source code changes. Authorization is based on role. C5-CA-06 – Network traffic within the Microsoft 365 environment is segregated to separate customer traffic from management traffic. C5-CA-07 – Cryptographic controls are used for information protection within the Microsoft 365 service based on the Microsoft 365 Cryptographic Policy and Key Management procedures. C5-CA-10 – M365 has established policies for mobile computing devices to meet appropriate security practices prior to being connected to the production environment.

Criteria	Microsoft 365 Control Activity
CC6.3 (continued) – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	*Complementary Subservice Organization Controls* **CSOC – 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. **CSOC – 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. **CSOC – Microsoft 365 Central –** Microsoft 365 Central service is responsible for maintaining controls over authentication and logical access. *Complementary User Entity Controls* **CUEC-01 –** User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access. **CUEC-06 –** User entities secure the software and hardware used to access M365.
CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	*Complementary Subservice Organization Controls* **CSOC – Microsoft Datacenters –** Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including data centers, supporting M365. Additionally, Microsoft Datacenters is responsible for maintaining controls for M365 that address environmental threats including natural disasters and man-made threats. **CSOC – Microsoft Datacenters –** Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including perimeter firewalls and restricting access to network devices. **CSOC – Microsoft Datacenters –** Microsoft Datacenters is responsible for maintaining controls over physical data storage, protection, and disposal services supporting M365.

Criteria	Microsoft 365 Control Activity
CC6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	CA-55 – Customer content is retained after termination of Microsoft 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements. *Complementary Subservice Organization Controls* CSOC – 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. CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including data centers, supporting M365. *Complementary User Entity Controls* CUEC-10 – User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality.
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CA-05 – The Governance, Risk, and Compliance team updates the data flow diagrams and service offerings of M365 with the individuals that act as point of contact for each service offering. CA-32 – Access to shared accounts within the Microsoft 365 environment are restricted to authorized personnel. CA-33.a – 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. CA-33.b – Elevated access within the M365 production environment is approved by an authorized user. CA-34 – Identity of users is authenticated to Microsoft 365 Services. The use of passwords incorporates policy on periodic change and password complexity. CA-35.a – Access to privileged accounts is configured to be revoked automatically based on access expiration settings, including inactivity and Manager / Cost Center changes. CA-35.b[4] – Elevated access within the M365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis. CA-36 – Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.

Criteria	Microsoft 365 Control Activity
CC6.6 (continued) – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	C5-CA-03 – Microsoft has policies documented to cover the management and provisioning of system and data access for the Microsoft 365 environment. Policies are communicated to M365 service teams and cover the following: - Provisioning of access - Separation of duties - Role/Eligibility approval process - Access termination - Required access control documentation C5-CA-04[5] – Cryptographic certificates, keys, and customer access keys used for communication between Azure and Microsoft 365 services and other internal components are stored securely. C5-CA-07 – Cryptographic controls are used for information protection within the Microsoft 365 service based on the Microsoft 365 Cryptographic Policy and Key Management procedures. C5-CA-10 – M365 has established policies for mobile computing devices to meet appropriate security practices prior to being connected to the production environment. C5-CA-19 – Microsoft 365 has security information and event management (SIEM) software that monitors logging data. Potential events are identified and reported to appropriate personnel for further evaluation as needed. C5-CA-20 – Microsoft 365 log data allows an unambiguous identification of user accesses to support further analysis in the event of a security incident. *Complementary Subservice Organization Controls* CSOC – 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. CSOC – 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. CSOC – Microsoft 365 Central – Microsoft 365 Central service is responsible for maintaining controls over authentication and logical access.

Criteria	Microsoft 365 Control Activity
CC6.6 (continued) – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	*Complementary User Entity Controls* **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-06 –** User entities secure the software and hardware used to access M365.
CC6.7 – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	**CA-36 –** Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment. **CA-37 –** Each Microsoft 365 Service Customer's content is segregated from other Online Services customers' content to isolate customer tenant data flows. **CA-44 –** Data in motion is encrypted when transmitting data between the customer and the data center and between data centers. **CA-45 –** Anti-malware detects and prevents introduction of known vulnerabilities and quarantines infected systems. Anti-malware signatures are updated as available. **CA-54 –** Data at rest is encrypted per policy. **CA-55 –** Customer content is retained after termination of Microsoft 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements. **C5-CA-04[5] –** Cryptographic certificates, keys, and customer access keys used for communication between Azure and Microsoft 365 services and other internal components are stored securely. **C5-CA-06 –** Network traffic within the Microsoft 365 environment is segregated to separate customer traffic from management traffic. **C5-CA-07 –** Cryptographic controls are used for information protection within the Microsoft 365 service based on the Microsoft 365 Cryptographic Policy and Key Management procedures. **C5-CA-08 –** Microsoft has policies and instructions documented to cover protection for data in motion, based on risk. Policies are communicated to M365 service teams. **C5-CA-12 –** Microsoft 365 customers are able to determine the locations where their data is being processed and stored via the M365 Administrator Tool.

Criteria	Microsoft 365 Control Activity
CC6.7 (continued) – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	*Complementary Subservice Organization Controls* **CSOC – 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. **CSOC – 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. **CSOC – Microsoft Azure –** Microsoft Azure is responsible for maintaining controls over data encryption for data at rest and in motion to the platform services supporting M365. **CSOC – Microsoft 365 Central –** Microsoft 365 Central service is responsible for maintaining controls over authentication and logical access. *Complementary User Entity Controls* **CUEC-02 –** User entities establish proper controls over the use of system IDs and passwords. **CUEC-04 –** User entities enforce desired level of encryption for network sessions. **CUEC-06 –** User entities secure the software and hardware used to access M365. **CUEC-10 –** User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality

Criteria	Microsoft 365 Control Activity
CC6.8 – The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	CA-38 – 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. CA-45 – Anti-malware detects and prevents introduction of known vulnerabilities and quarantines infected systems. Anti-malware signatures are updated as available. CA-46 – Production releases undergo a security review prior to their release into the production environment per defined criteria, including a code review. C5-CA-14 – Administrator activity in the Microsoft 365 environment is logged. C5-CA-19 – Microsoft 365 has security information and event management (SIEM) software that monitors logging data. Potential events are identified and reported to appropriate personnel for further evaluation as needed. *Complementary Subservice Organization Controls* CSOC – Microsoft 365 Central – Microsoft 365 Central service is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management. CSOC – 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. *Complementary User Entity Controls* CUEC-06 – User entities secure the software and hardware used to access M365.

CC7.0 – Common Criteria Related to Systems Operations

Criteria	Microsoft 365 Control Activity
CC7.1 – To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	CA-01 – A Microsoft 365 security team has been defined and is responsible for Security issues within the Microsoft 365 environment. Service teams have operations personnel who are responsible for system operation and service availability. CA-21 – Testing is carried out on all changes according to established procedures. Users and stakeholders review and approve results of testing prior to implementation. CA-29 – Each Service team has on-call personnel who respond to potential Security, availability, confidentiality, and processing integrity incidents. If an incident is assigned a high severity, the M365 Security team will track and address the issues to resolution. CA-30[6] – Processing capacity and availability are monitored by Service teams through the dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed. CA-38 – 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. CA-45 – Anti-malware detects and prevents introduction of known vulnerabilities and quarantines infected systems. Anti-malware signatures are updated as available. CA-46 – Production releases undergo a security review prior to their release into the production environment per defined criteria, including a code review. C5-CA-14 – Administrator activity in the Microsoft 365 environment is logged. C5-CA-15 – The access and management of the logging and monitoring functionalities is limited to select personnel. Changes to the logging and monitoring are approved by the engineering teams. C5-CA-19 – Microsoft 365 has security information and event management (SIEM) software that monitors logging data. Potential events are identified and reported to appropriate personnel for further evaluation as needed. C5-CA-20 – Microsoft 365 log data allows an unambiguous identification of user accesses to support further analysis in the event of a security incident.

[6] M365 management noted that there was no occurrence for this control for OMAHA and M365 Remote Help.

Criteria	Microsoft 365 Control Activity
CC7.1 (continued) – To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	*Complementary Subservice Organization Controls* CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management for M365 services hosted on the Azure platform. CSOC – 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. CSOC – Microsoft 365 Central – Microsoft 365 Central service is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management. *Complementary User Entity Controls* CUEC-06 – User entities secure the software and hardware used to access M365.

Criteria	Microsoft 365 Control Activity
CC7.2 – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	CA-29 – Each Service team has on-call personnel who respond to potential Security, availability, confidentiality, and processing integrity incidents. If an incident is assigned a high severity, the M365 Security team will track and address the issues to resolution. CA-30[6] – Processing capacity and availability are monitored by Service teams through the dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed. CA-38 – 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. CA-50 – 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. CA-53 – Microsoft 365 monitors its dependencies on third parties through obtaining and evaluating attestation reports when available. C5-CA-14 – Administrator activity in the Microsoft 365 environment is logged. C5-CA-16 – Microsoft participates in penetration testing of key components of the Microsoft 365 environment. Results of the penetration tests are documented and any critical findings are remedied. C5-CA-19 – Microsoft 365 has security information and event management (SIEM) software that monitors logging data. Potential events are identified and reported to appropriate personnel for further evaluation as needed. C5-CA-20 – Microsoft 365 log data allows an unambiguous identification of user accesses to support further analysis in the event of a security incident.

Criteria	Microsoft 365 Control Activity
CC7.2 (continued) – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	*Complementary Subservice Organization Controls* **CSOC – Microsoft Azure** – Microsoft Azure is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management for M365 services hosted on the Azure platform. **CSOC – 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. **CSOC – Microsoft Azure –** Microsoft Azure is responsible for maintaining controls over data encryption for data at rest and in motion to the platform services supporting M365. **CSOC – Microsoft 365 Central –** Microsoft 365 Central service is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management. *Complementary User Entity Controls* **CUEC-07** – User entities conduct end-user training. **CUEC-08 –** User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.

Criteria	Microsoft 365 Control Activity
CC7.3 – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing M365 and prioritize the most preeminent risks based on impact, likelihood, and management's controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by M365 management with ownership assigned out to individual teams and their management. CA-23 – Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis. CA-29 – Each Service team has on-call personnel who respond to potential Security, availability, confidentiality, and processing integrity incidents. If an incident is assigned a high severity, the M365 Security team will track and address the issues to resolution. CA-38 – 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. ELC-09 – Microsoft's Enterprise Business Continuity program is intended to ensure that Microsoft is ready to mitigate risks and vulnerabilities and respond to a major disruptive event in a manner that enables the business to continue to operate in a safe, predictable, and reliable way. The EBCM charter provides a strategic direction and leadership to all Microsoft Engineering organizations. EBCM is governed through the Program Management Office to ensure that the program adheres to a coherent long-term vision and mission, and is consistent with enterprise program standards, methods, policies, and metrics. *Complementary Subservice Organization Controls* CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management for M365 services hosted on the Azure platform. CSOC – 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. CSOC – Microsoft 365 Central – Microsoft 365 Central service is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management. *Complementary User Entity Controls* CUEC-08 – User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.

Criteria	Microsoft 365 Control Activity
CC7.4 – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	CA-01 – A Microsoft 365 security team has been defined and is responsible for Security issues within the Microsoft 365 environment. Service teams have operations personnel who are responsible for system operation and service availability. CA-13 – Incident response guides are used by Microsoft 365 personnel for the handling and reporting of security incidents. These guides are stored on internal SharePoint sites and are updated as needed. CA-17 – Microsoft 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) compromised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet. CA-21 – Testing is carried out on all changes according to established procedures. Users and stakeholders review and approve results of testing prior to implementation. CA-29 – Each Service team has on-call personnel who respond to potential Security, availability, confidentiality, and processing integrity incidents. If an incident is assigned a high severity, the M365 Security team will track and address the issues to resolution. *Complementary Subservice Organization Controls* CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management for M365 services hosted on the Azure platform. CSOC – 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. CSOC – Microsoft 365 Central – Microsoft 365 Central service is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management. *Complementary User Entity Controls* CUEC-08 – User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.

Criteria	Microsoft 365 Control Activity
CC7.5 – The entity identifies, develops, and implements activities to recover from identified security incidents.	CA-01 – A Microsoft 365 security team has been defined and is responsible for Security issues within the Microsoft 365 environment. Service teams have operations personnel who are responsible for system operation and service availability. CA-13 – Incident response guides are used by Microsoft 365 personnel for the handling and reporting of security incidents. These guides are stored on internal SharePoint sites and are updated as needed. CA-17 – Microsoft 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) compromised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet. CA-29 – Each Service team has on-call personnel who respond to potential Security, availability, confidentiality, and processing integrity incidents. If an incident is assigned a high severity, the M365 Security team will track and address the issues to resolution. ELC-09 – Microsoft's Enterprise Business Continuity program is intended to ensure that Microsoft is ready to mitigate risks and vulnerabilities and respond to a major disruptive event in a manner that enables the business to continue to operate in a safe, predictable, and reliable way. The EBCM charter provides a strategic direction and leadership to all Microsoft Engineering organizations. EBCM is governed through the Program Management Office to ensure that the program adheres to a coherent long-term vision and mission, and is consistent with enterprise program standards, methods, policies, and metrics. *Complementary Subservice Organization Controls* CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management for M365 services hosted on the Azure platform.

Criteria	Microsoft 365 Control Activity
CC7.5 (continued) – The entity identifies, develops, and implements activities to recover from identified security incidents.	CSOC – 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. CSOC – Microsoft 365 Central – Microsoft 365 Central service is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management. *Complementary User Entity Controls* CUEC-08 – User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues. CUEC-10 – User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality.

CC8.0 – Common Criteria Related to Change Management

Criteria	Microsoft 365 Control Activity
CC8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CA-03 – Senior Management, as part of its major system release planning process, considers its commitments and requirements for Security, availability, confidentiality, and processing integrity. CA-11 – On an annual basis services are updated to reflect changes made to the Microsoft 365 control framework. CA-14 – Changes and updates to the M365 environment are communicated through the admin Message Center part of the M365 Admin Center. CA-18 – Changes and software releases within the Microsoft 365 environment are documented / tracked and are approved prior to implementation into production. CA-19 – For teams utilizing the Developer / Operations model, monitoring processes or system configurations are in place to identify and remediate unapproved changes to production. CA-20[7] – Emergency changes to the production environment follow an emergency change approval process. CA-21 – Testing is carried out on all changes according to established procedures. Users and stakeholders review and approve results of testing prior to implementation. CA-46 – Production releases undergo a security review prior to their release into the production environment per defined criteria, including a code review. C5-CA-02 – In case of errors or security concerns, changes are rolled back to their previous state or rolled forward to a corrected state. C5-CA-05 – Code repositories are used for managing source code changes to the Microsoft 365 platform. Procedures are established for authorized M365 personnel to submit source code changes. Authorization is based on role. C5-CA-15 – The access and management of the logging and monitoring functionalities is limited to select personnel. Changes to the logging and monitoring are approved by the engineering teams.

[7] M365 management noted that there was no occurrence for this control for IDEAs Delivery Service (IDS) and OMAHA.

CC9.0 – Common Criteria Related to Risk Mitigation

Criteria	Microsoft 365 Control Activity
CC9.1 – The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing M365 and prioritize the most preeminent risks based on impact, likelihood, and management's controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by M365 management with ownership assigned out to individual teams and their management. CA-23 – Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis. CA-24 – Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner. CA-50 – 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. CA-51 – Customer content and services are replicated to a geographically separate location. C5-CA-16 – Microsoft participates in penetration testing of key components of the Microsoft 365 environment. Results of the penetration tests are documented and any critical findings are remedied. C5-CA-17 – Microsoft 365 performs an annual Information Security Management System (ISMS) reviews and reviews results with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. C5-CA-18 – Microsoft 365 has a defined exception program where exceptions are reviewed and tracked. The results of the review process are documented, and if approved the exception is limited in time and reviewed at least annually by relevant risk owners. C5-CA-19 – Microsoft 365 has security information and event management (SIEM) software that monitors logging data. Potential events are identified and reported to appropriate personnel for further evaluation as needed. C5-CA-22 – Procedures are established and documented to evaluate government investigative demands for customer data. Procedures address a review and assessment by the Microsoft legal department, which will evaluate the legal basis for the request to determine what response is required, notify the impacted customer where permitted by law, where Microsoft is required to produce customer data, work with engineering to collect and produce the minimum data responsive to the request as required by law. Procedures are reviewed at least annually.

Criteria	Microsoft 365 Control Activity
CC9.1 (continued) – The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	**ELC-09** – Microsoft's Enterprise Business Continuity program is intended to ensure that Microsoft is ready to mitigate risks and vulnerabilities and respond to a major disruptive event in a manner that enables the business to continue to operate in a safe, predictable, and reliable way. The EBCM charter provides a strategic direction and leadership to all Microsoft Engineering organizations. EBCM is governed through the Program Management Office to ensure that the program adheres to a coherent long-term vision and mission, and is consistent with enterprise program standards, methods, policies, and metrics. *Complementary Subservice Organization Controls* **CSOC – Microsoft Azure –** Microsoft Azure is responsible for maintaining controls over data replication and redundancy to the platform services supporting M365. **CSOC – Microsoft Datacenters –** Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including data centers, supporting M365. Additionally, Microsoft Datacenters is responsible for maintaining controls for M365 that address environmental threats including natural disasters and man-made threats.
CC9.2 – The entity assesses and manages risks associated with vendors and business partners.	**CA-22 –** Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing M365 and prioritize the most preeminent risks based on impact, likelihood, and management's controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by M365 management with ownership assigned out to individual teams and their management. **CA-23 –** Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis. **CA-24 –** Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner. **CA-53 –** Microsoft 365 monitors its dependencies on third parties through obtaining and evaluating attestation reports when available. **C5-CA-17 –** Microsoft 365 performs an annual Information Security Management System (ISMS) reviews and reviews results with management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.

Criteria	Microsoft 365 Control Activity
CC9.2 (continued) – The entity assesses and manages risks associated with vendors and business partners.	C5-CA-18 – Microsoft 365 has a defined exception program where exceptions are reviewed and tracked. The results of the review process are documented, and if approved the exception is limited in time and reviewed at least annually by relevant risk owners. C5-CA-21 – Prior to contracting with Microsoft, suppliers undergo a risk assessment based on the services that will be provided and data handled. List of reviewed suppliers is maintained and their risk profiles are reviewed at least annually. ELC-08 – Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, including the consequences of violating relevant laws, regulations, provisions, and policies regarding information security. Employees are required to acknowledge agreements to return Microsoft assets upon termination. ELC-12 – Management expects outsourced providers to meet certain levels of skills and experience, depending on the role and holds them accountable to achieving specific deliverables, as outlined in a Statement of Work. Outsourced providers are trained to understand and comply with Microsoft's supplier code of conduct. ELC-15 – Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Microsoft 365 environment based on Microsoft's corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements. *Complementary User Entity Controls* CUEC-07 – User entities conduct end-user training. CUEC-08 – User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.

Additional Criteria for Availability

Criteria	Microsoft 365 Control Activity
A1.1 – The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	CA-29 – Each Service team has on-call personnel who respond to potential Security, availability, confidentiality, and processing integrity incidents. If an incident is assigned a high severity, the M365 Security team will track and address the issues to resolution. CA-30[6] – Processing capacity and availability are monitored by Service teams through the dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed. CA-31 – Microsoft 365 management reviews capacity and availability on a monthly basis. Any issues with or changes to capacity and availability are tracked to resolution.
A1.2 – The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	CA-29 – Each Service team has on-call personnel who respond to potential Security, availability, confidentiality, and processing integrity incidents. If an incident is assigned a high severity, the M365 Security team will track and address the issues to resolution. CA-49 – Procedures have been established for local redundant storage and/or other redundancy measures supporting the availability of applications and customer content. CA-50 – 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. CA-51 – Customer content and services are replicated to a geographically separate location. C5-CA-12 – Microsoft 365 customers are able to determine the locations where their data is being processed and stored via the M365 Administrator Tool. C5-CA-16 – Microsoft participates in penetration testing of key components of the Microsoft 365 environment. Results of the penetration tests are documented and any critical findings are remedied. *Complementary Subservice Organization Controls* CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including datacenters, supporting M365. Additionally, Microsoft Datacenters is responsible for maintaining controls for M365 that address environmental threats including natural disasters and man-made threats. CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over data replication and redundancy to the platform services supporting M365. *Complementary User Entity Controls* CUEC-06 – User entities secure the software and hardware used to access M365.

Criteria	Microsoft 365 Control Activity
A1.3 – The entity tests recovery plan procedures supporting system recovery to meet its objectives.	CA-49 – Procedures have been established for local redundant storage and/or other redundancy measures supporting the availability of applications and customer content. CA-50 – Service teams participate in Business Continuity programs, which specify, based on criticality, recovery objectives, testing requirements (up to full datacenter failover), and remediation timelines. CA-51 – Customer content and services are replicated to a geographically separate location. C5-CA-16 – Microsoft participates in penetration testing of key components of the Microsoft 365 environment. Results of the penetration tests are documented and any critical findings are remedied. *Complementary Subservice Organization Controls* CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including datacenters, supporting M365. Additionally, Microsoft Datacenters is responsible for maintaining controls for M365 that address environmental threats including natural disasters and man-made threats. CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over data replication and redundancy to the platform services supporting M365.

Additional Criteria for Processing Integrity

Criteria	Microsoft 365 Control Activity
PI1.1 – The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	CA-02 – A Microsoft 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, availability, confidentiality, and processing integrity controls within the Microsoft 365 environment. CA-12 – Microsoft 365 communicates its commitments to customers in SLAs. These commitments are reflected in the control framework, which defines regulatory, security, availability, confidentiality, and processing integrity requirements. This information is distributed internally through policies, training, and Office Hours. CA-66 – Production data is classified and protected based upon the Microsoft 365 data classification process. C5-CA-01 – Microsoft has policies documented to cover the development of information systems within the Microsoft 365 environment. Policies are communicated to M365 service teams and cover the following: - Security standards - Security Development Lifecycle - Version control - Programming policies C5-CA-12 – Microsoft 365 customers are able to determine the locations where their data is being processed and stored via the M365 Administrator Tool. *Complementary User Entity Controls* CUEC-08 – User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues. CUEC-10 – User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality. CUEC-12 – User entities are responsible for managing their data processing within M365 for completeness, accuracy, and timeliness.

Criteria	Microsoft 365 Control Activity
PI1.2 – The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	CA-02 – A Microsoft 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, availability, confidentiality, and processing integrity controls within the Microsoft 365 environment. CA-12 – Microsoft 365 communicates its commitments to customers in SLAs. These commitments are reflected in the control framework, which defines regulatory, security, availability, confidentiality, and processing integrity requirements. This information is distributed internally through policies, training, and Office Hours. C5-CA-13 – (1) Microsoft has policies and instructions documented to communicate the secure collection and storage of metadata within the Microsoft 365 environment. Policies are communicated to M365 service teams. (2) Metadata is collected and used in accordance with contractual commitments. *Complementary User Entity Controls* CUEC-11 – User entities are responsible for managing their data inputs, and data uploads to M365 for completeness, accuracy, and timeliness. CUEC-12 – User entities are responsible for managing their data processing within M365 for completeness, accuracy, and timeliness.
PI1.3 – The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.	CA-12 – Microsoft 365 communicates its commitments to customers in SLAs. These commitments are reflected in the control framework, which defines regulatory, security, availability, confidentiality, and processing integrity requirements. This information is distributed internally through policies, training, and Office Hours. CA-30[6] – Processing capacity and availability are monitored by Service teams through the dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed. CA-31 – Microsoft 365 management reviews capacity and availability on a monthly basis. Any issues with or changes to capacity and availability are tracked to resolution. CA-49 – Procedures have been established for local redundant storage and/or other redundancy measures supporting the availability of applications and customer content. CA-51 – Customer content and services are replicated to a geographically separate location. C5-CA-13 – (1) Microsoft has policies and instructions documented to communicate the secure collection and storage of metadata within the Microsoft 365 environment. Policies are communicated to M365 service teams. (2) Metadata is collected and used in accordance with contractual commitments. *Complementary User Entity Controls* CUEC-12 – User entities are responsible for managing their data processing within M365 for completeness, accuracy, and timeliness.

Criteria	Microsoft 365 Control Activity
PI1.4 – The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.	CA-12 – Microsoft 365 communicates its commitments to customers in SLAs. These commitments are reflected in the control framework, which defines regulatory, security, availability, confidentiality, and processing integrity requirements. This information is distributed internally through policies, training, and Office Hours. CA-30[6] – Processing capacity and availability are monitored by Service teams through the dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed. CA-31 – Microsoft 365 management reviews capacity and availability on a monthly basis. Any issues with or changes to capacity and availability are tracked to resolution. C5-CA-11 – Customer data is accessible within agreed upon services in data formats compatible with providing those services. C5-CA-13 – (1) Microsoft has policies and instructions documented to communicate the secure collection and storage of metadata within the Microsoft 365 environment. Policies are communicated to M365 service teams. (2) Metadata is collected and used in accordance with contractual commitments. *Complementary User Entity Controls* CUEC-14 – User entities are responsible for managing their data output from M365 for completeness, accuracy, and timeliness.

Criteria	Microsoft 365 Control Activity
PI1.5 – The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.	CA-33.a – 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. CA-33.b – Elevated access within the M365 production environment is approved by an authorized user. CA-35.a – Access to privileged accounts is configured to be revoked automatically based on access expiration settings, including inactivity and Manager / Cost Center changes. CA-35.b[4] – Elevated access within the M365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis. CA-51 – Customer content and services are replicated to a geographically separate location. CA-55 – Customer content is retained after termination of Microsoft 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements. C5-CA-11 – Customer data is accessible within agreed upon services in data formats compatible with providing those services. C5-CA-12 – Microsoft 365 customers are able to determine the locations where their data is being processed and stored via the M365 Administrator Tool. C5-CA-13 – (1) Microsoft has policies and instructions documented to communicate the secure collection and storage of metadata within the Microsoft 365 environment. Policies are communicated to M365 service teams. (2) Metadata is collected and used in accordance with contractual commitments. *Complementary Subservice Organization Controls* CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over data encryption for data at rest and in motion to the platform services supporting M365. CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over physical data storage, protection, and disposal services supporting M365. *Complementary User Entity Controls* CUEC-10 – User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality. CUEC-13 – User entities are responsible for managing their stored data for completeness and accuracy.

Additional Criteria for Confidentiality

Criteria	Microsoft 365 Control Activity
C1.1 – The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	CA-43 – When users no longer require access or upon termination the user access privileges are revoked in a timely manner. CA-44 – Data in motion is encrypted when transmitting data between the customer and the data center and between data centers. CA-54 – Data at rest is encrypted per policy. CA-55 – Customer content is retained after termination of Microsoft 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements. CA-66 – Production data is classified and protected based upon the Microsoft 365 data classification process. C5-CA-04[5] – Cryptographic certificates, keys, and customer access keys used for communication between Azure and Microsoft 365 services and other internal components are stored securely. C5-CA-07 – Cryptographic controls are used for information protection within the Microsoft 365 service based on the Microsoft 365 Cryptographic Policy and Key Management procedures. C5-CA-08 – Microsoft has policies and instructions documented to cover protection for data in motion, based on risk. Policies are communicated to M365 service teams. C5-CA-12 – Microsoft 365 customers are able to determine the locations where their data is being processed and stored via the M365 Administrator Tool. *Complementary Subservice Organization Controls* CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over data encryption for data at rest and in motion to the platform services supporting M365. CSOC – Microsoft Datacenters- Microsoft Datacenters is responsible for maintaining controls over physical data storage, protection, and disposal services supporting M365. *Complementary User Entity Controls* CUEC-04 – User entities enforce desired level of encryption for network sessions.
C1.2 – The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	CA-55 – Customer content is retained after termination of Microsoft 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements. CA-66 – Production data is classified and protected based upon the Microsoft 365 data classification process.

Section 4:
Supplemental Information Provided by Management of Microsoft

Section 4: Supplemental Information Provided by Management of Microsoft

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

Business Continuity Planning

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

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

Domain Name Services

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

Datacenter Services

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

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

ISO/IEC Standards 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 27017:2015, 27018:2019, and 27701:2019 published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). M365 is also compliant with ISO standard 22301:2019.

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 undergone the ISO 27001 certification and service has been certified by the British Standards Institute (BSI). To view the ISO/IEC 27001:2022 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.

Management's Response to Exceptions Identified

The table below contains Management's responses to the exceptions identified.

Control Activity & Exception	Management's Response
CA-35.b - Elevated access within the M365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis. Productivity Applications and Services One relevant group was not included in the User Access Review for the sampled quarter from for the Tasks – Business Scenario Service. Bing Teams No exceptions noted during Deloitte & Touche LLP's testing. However, Internal Audit (IA) noted that for the Microsoft Search in Bing (MSB) team, 2 of 8 security groups with privileged repository access were not reviewed. The access was not reviewed. The access for all users within the security groups was deemed appropriate.	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.
C5-CA-04 – Cryptographic certificates, keys, and customer access keys used for communication between Azure and Microsoft 365 services and other internal components are stored securely. Bookings Odata API Per inquiry with management, noted that the company did not retain evidence for testing of this control.	The Bookings Odata API service is deprecating and therefore evidence was not retained for control C5-CA-04 in this report. This did not result in any gaps in Booking's ability to meet service commitments or the SOC criteria covered by the scope of this report.

Controls Not Subject to this Examination

Control Activity	Implementation Evaluation
CA-20 - Emergency changes to the production environment follow an emergency change approval process.	No Occurrence (IDEAs Delivery Service (IDS) and OMAHA) M365 management noted that there was no occurrence for this control for IDEAs Delivery Service (IDS) and OMAHA.
CA-30 - Processing capacity and availability are monitored by Service teams through the dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed.	No Occurrence (OMAHA and M365 Remote Help) M365 management noted that there was no occurrence for this control for OMAHA and M365 Remote Help.