Microsoft

Microsoft Corporation—Office 365

System and Organization Controls (SOC) 2 Report

October 1, 2019 through September 30, 2020

Deloitte.

Table of Contents

Executive Summary

Microsoft Corporation—Office 365	
Scope	Microsoft Office 365 (O365) including Office 365 with International Traffic in Arms Regulations (ITAR)[1] Support
Period of Examination	October 1, 2019 through September 30, 2020
Location(s)	Redmond, WA
Subservice Providers	Yes – • Microsoft Azure ("Azure") including Microsoft Datacenters
Opinion Result	Unqualified
Testing Exceptions	3 – See **Pages 93 and 97**
Complementary User-Entity Controls	Yes – See **Page 32**
Complementary Subservice Organization Controls	Yes – See **Page 34**

[1] This report is a description of the "Microsoft Office 365 with ITAR Support system" (O365) as defined in the system description. The inclusion of the ITAR reference in the formal name of the system is not intended to examine or opine on the requirements of the United States International Traffic in Arms Regulations (ITAR).

Section I:
Independent Service Auditor’s Report

Deloitte.

Deloitte & Touche LLP

925 4th Avenue, Suite 3300
Seattle, WA 98104
USA
Tel: 206 716 7000
Fax: 206 965-7000
www.deloitte.com

Section I:
Independent Service Auditor's Report

Microsoft Corporation
Redmond, Washington, 98052

Scope

We have examined the attached description of the system of Microsoft Corporation (the "Service Organization" or "Microsoft") related to its Microsoft Office 365, including International Traffic in Arms Regulations (ITAR)[2] Support, online services for processing user entities' transactions for the period October 1, 2019, to September 30, 2020 (the "Description") based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and processing integrity ("applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

The information in **Section V**, "Supplemental information provided by Microsoft," is presented by management of the Service Organization to provide additional information and is not a part of the Description. Information presented in **Section V** has not been subjected to the procedures applied in the examination of the Description and the suitability of the design and operating effectiveness of controls to achieve the Service Organization's service commitments and system requirements based on the applicable trust services criteria.

The Service Organization uses Microsoft Azure including the Microsoft Datacenter service ("subservice organization") for its hosting of physical and virtual servers, network management, and data protection and storage services. The Description indicates that complementary subservice organization controls that are suitably designed 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 the Service Organization's controls; the applicable trust services criteria; and the types of complementary subservice organization controls assumed in the design of the Service Organization's controls. The Description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated whether the controls management expects to be implemented at the subservice organization have been implemented or whether such controls were suitability designed and operating effectively throughout the period October 1, 2019, to September 30, 2020.

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

[2] This report is a description of the "Microsoft Office 365 with ITAR Support system" (O365) as defined in the system description. The inclusion of the ITAR reference in the formal name of the system is not intended to examine or opine on the requirements of the United States International Traffic in Arms Regulations (ITAR).

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 include 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

The Service Organization 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 the Service Organization's service commitments and system requirements were achieved. The Service Organization has provided the accompanying assertion titled "Management's assertion" ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. The Service Organization 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 the design and operating effectiveness of the 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 3000, *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our 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 and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were 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 the description of a service organization's system and the suitability of the design and operating effectiveness of those controls involves the following:

- 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 or did not operate effectively.
- 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 achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of those controls stated in the description to provide reasonable assurance that the service organization achieved 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 have complied with the independence and other ethical requirements of the *Code of Professional Conduct* established by the AICPA. We applied the statements on quality control standards established by the AICPA, 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 may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization’s service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of the 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.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of our tests are listed in Section IV of this report.

Opinion

In our opinion, in all material respects,

a. The Description presents the O365 online services system of Microsoft that was designed and implemented throughout the period October 1, 2019, to September 30, 2020, in accordance with the description criteria.

b. The controls stated in the Description were suitably designed throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Microsoft’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period and the subservice organization and user entities applied the complementary controls assumed in the design of the Service Organization’s controls throughout that period.

c. The controls stated in the Description operated effectively throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Microsoft’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and user entity controls assumed in the design of the Service Organization’s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Microsoft, user entities of the in-scope services for Microsoft’s O365 online services system during some or all of the period October 1, 2019, to September 30, 2020, business partners of Microsoft subject to risks arising from interactions with Microsoft’s O365 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 the Service Organization.

- How the Service Organization’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 the Service Organization to achieve the Service Organization’s commitments and system requirements.
- User entity responsibilities and how they may affect the user entity’s ability to effectively use the Service Organization’s services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization’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

December 24, 2020

Section II:
Management’s Assertion

Section II:
Management's Assertion

Microsoft Corporation's Assertion

We have prepared the description of the system in **Section III** of Microsoft Corporation ("Service Organization", "Microsoft") throughout the period October 1, 2019, to September 30, 2020 (the "period"), related to its Microsoft Office 365, including Office 365 with International Traffic in Arms Regulations (ITAR)[3] Support, online services ("O365"), based on 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 ("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, confidentiality, and processing integrity set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy ("applicable trust services criteria").

The Service Organization uses Microsoft Azure including the Microsoft Datacenter service ("subservice organization") for its hosting of physical and virtual servers, network management, and data protection and storage. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls for O365, to achieve Microsoft's service commitments and system requirements related to O365 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 organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Microsoft to achieve the service commitments and system requirements related to O365 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.

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

a. The description presents Microsoft's system that was designed and implemented throughout the period October 1, 2019, to September 30, 2020, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Microsoft's service commitments and system requirements related to O365 would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Microsoft's controls throughout that period.

[3] This report is a description of the "Microsoft Office 365 with ITAR Support system" (O365) as defined in the system description. The inclusion of the ITAR reference in the formal name of the system is not intended to examine or opine on the requirements of the United States International Traffic in Arms Regulations (ITAR).

c. The controls stated in the description operated effectively throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Microsoft's service commitments and system requirements would be achieved based on the applicable trust services criteria, if complementary subservice organization and user entity controls assumed in the design of Microsoft operated effectively throughout that period.

Section III:
Description of the System

Section III:
Description of the System

Overview of Operations

Business Description

Microsoft Corporation's ("Microsoft") Office 365 ("O365") service is a subscription-based business software service hosted by Microsoft and sold directly, or with partners, to various customers worldwide. O365 services are designed to provide performance, scalability, security, management capabilities, and service levels required for mission-critical applications and systems used by business organizations.

Customers subscribe to a standard set of features and services which are hosted in a shared, multi-tenant environment. This includes the Government Community Cloud, an Office 365 offering designed for US government customers. Also included is the Government Community Cloud High and Department of Defense offering, in which customers subscribe to a standard set of features hosted in a multi-tenant environment designed for the US Federal government, defense industry, aerospace industry, and government contractors to provide United States International Traffic in Arms Regulations (ITAR) support and meet Defense Information Systems Agency requirements.

O365 is physically hosted in Microsoft-managed datacenters. Microsoft Datacenters is an organization within Microsoft that provides hosting and network support solutions for the O365 environment. Microsoft Azure ("Azure") is an organization within Microsoft that provides supporting services for the O365 applications including authentication, virtual server hosting, and system data storage and protection. Microsoft Datacenters is managed and run by Azure and both services are treated as one subservice organization (Azure) but will be referred to separately in this report to clarify which part of the Azure organization is responsible for the different services. Both services are not within the scope of this report.

The following services are provided to all O365 customers:

- Email access and productivity tools
- Team communication and collaboration
- Document and other file storage
- Documents viewed and edited in a Web browser

Additionally, O365 streamlines workflow for customers by providing them with added security, increased email accessibility, and easy team collaboration by providing hosted messaging and collaboration solutions.

Applicability of the Report

This report has been prepared to provide information on O365's internal controls that may be relevant to the requirements of its customers and affect the processing of user entities' transactions. The detail herein is intended to meet the common requirements of a broad range of users and may not, therefore, include every aspect of the system that each customer may consider important. Furthermore, detail is limited to the controls in operation over the system as defined in the O365 scope boundary described below. The authorized users of the system supporting the internal controls are limited to O365 personnel. This report covers the software offerings described in the sections below.

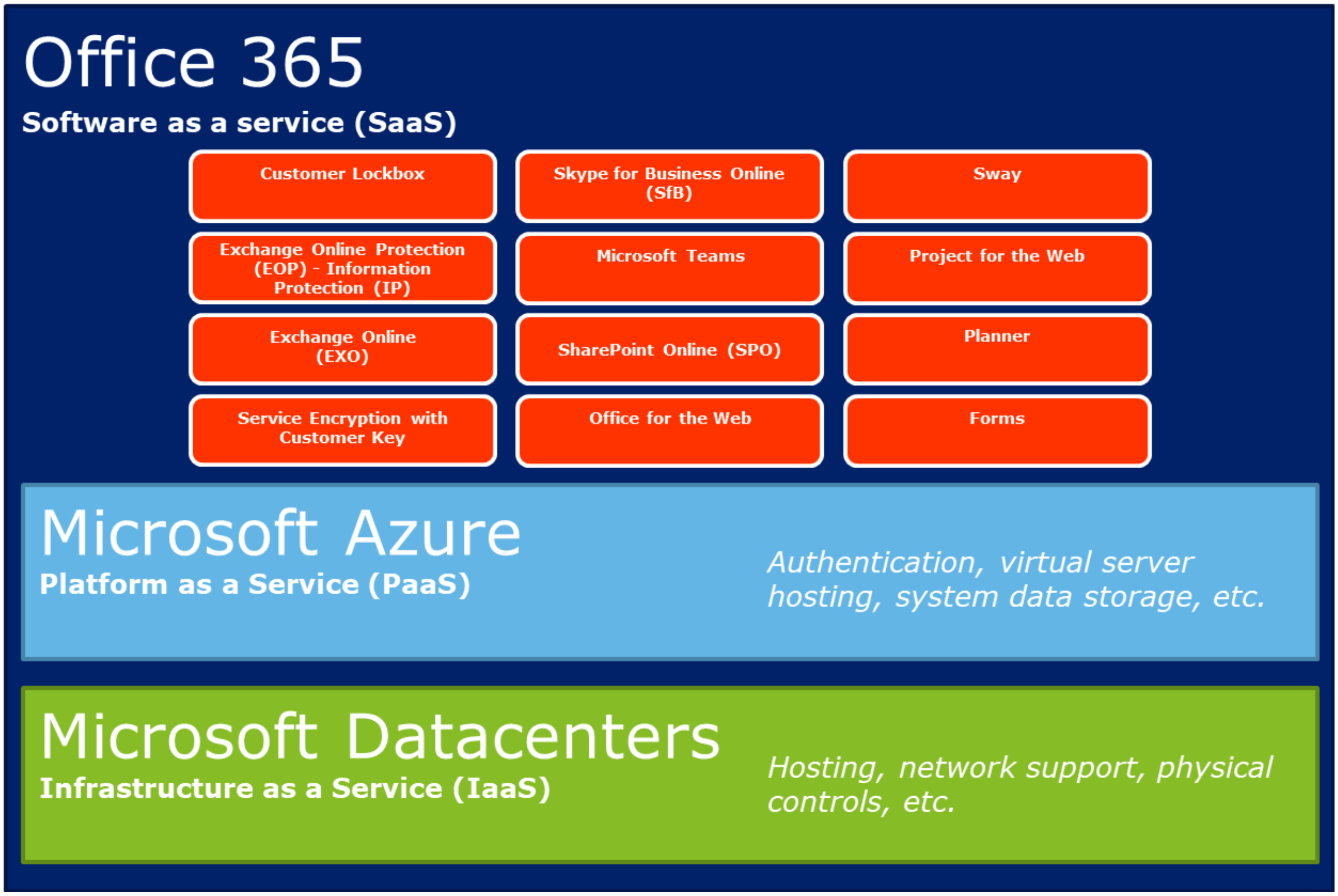
Infrastructure

All O365 services are hosted on a combination of the following subservice organizations within Microsoft: Microsoft Datacenters Infrastructure as a Service (IaaS) and Azure's IaaS and Platform as a Service (PaaS).

For Microsoft Datacenters hosting, the physical servers are owned by O365, the operating system (OS) and software are managed by O365, and network layer and network layer protections are implemented by Microsoft Datacenters. O365 manages the configuration of the network layer/protection in coordination with Microsoft Datacenters.

For Azure's IaaS hosting, O365 is responsible for the OS and database management. For Azure PaaS hosting, O365 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. Additionally, Azure manages the gateways for remote access into the O365 networks.

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 and Azure are not in the scope of this report.


Office 365
Software as a service (SaaS)
Customer Lockbox
Skype for Business Online (SfB)
Sway
Exchange Online Protection (EOP) - Information Protection (IP)
Microsoft Teams
Project for the Web
Exchange Online (EXO)
SharePoint Online (SPO)
Planner
Service Encryption with Customer Key
Office for the Web
Forms
Microsoft Azure
Platform as a Service (PaaS)
Authentication, virtual server hosting, system data storage, etc.
Microsoft Datacenters
Infrastructure as a Service (IaaS)
Hosting, network support, physical controls, etc.

Software

O365 includes the following SaaS offerings:

- Customer Lockbox – An access control technology designed to provide customer control and transparency over access to customer content.

- Exchange Online Protection (EOP) - Information Protection (IP) – A service providing security features, such as antivirus, antimalware, and antispam filtering for Exchange.
- Exchange Online (EXO) – An email service.
- Service Encryption with Customer Key – A service providing customers with two application-level encryption options for customer content at rest within the Exchange and SharePoint environments: Service Encryption with Microsoft-owned encryption keys and Service Encryption with customer-owned encryption keys ("Customer Keys").
- Skype for Business Online (SfB) – A communication service that offers collaboration capabilities via instant messaging, audio and video calling, online meetings, and web conferencing.
- Microsoft Teams – A communication service that offers a threaded persistent chat experience that builds on O365's group infrastructure, global scale, enterprise grade security, and graph driven intelligence.
- SharePoint Online (SPO) – A solution for creating websites to share documents and information with colleagues and customers. This information and documentation repository includes OneDrive, Delve, Access Online, and Project Online.
- Office for the Web (formally Office Online) – Enables users to access, view, and edit documents online via a web browser.
- Sway – Digital storytelling app for creating interactive reports, presentations, personal stories, and more.
- Project for the Web – Cloud-based work and project management.
- Planner – Provides a visual way to organize teamwork and simplified task management.
- Forms – Create surveys, quizzes, and polls with real-time results, built-in response analytics, and export to Excel.

O365 uses the following software to support the above offerings:

- Microsoft 365 (M365) Remote Access – A set of servers providing remote access to O365 service production environments via authorized two-factor authentication and encryption. This service was deprecated during the audit period and replaced with Azure Gateway, which is managed by the Azure subservice organization.
- Identity Manager (IDM) – An access management service providing an integrated and broad solution for managing O365 user identities and associated credentials for all O365 services (with the exception Microsoft Teams, which leverages MyAccess).

In addition to the product software, the following utilities are used by the service teams to execute controls relevant to the O365 system but are not directly covered in this report:

- 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.
- Beyond Trust (BT) – Scanning systems used to identify and resolve security vulnerabilities within the O365 environment.
- CorpFIM/IDWeb, MyAccess, and Torus – O365 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 O365 environment remotely using Azure Gateway managed Remote Desktop Gateways (RDGs).

- Griffin/Office Supporting Infrastructure, Office Substrate Pulse (OSP), O365SuiteUX Environments and Release Dashboard, PilotFish, and Azure DevOps – Change management tools used by service and support teams to track and deploy code changes to production environments.
- Aria, Avocado, Geneva, Incident Manager (IcM), Jarvis, and Heat Map – 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.
- Torus – An internal tool that restricts user access to production environments through creating and managing separate authorized accounts accessible via gateway servers.

People

O365 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 O365 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.
- Change Management – Development, testing, and project management teams tasked with developing and maintaining the O365 applications and supporting services.
- Backups and Replication – Personnel for configuring and monitoring the replication and backup of specified internal and customer content.
- Security and Availability Monitoring – Personnel that monitor the incidents that affect the security and availability of O365 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 O365 teams in analyzing continuity and disaster recovery requirements, documenting procedures, and conducting testing of established procedures.
- O365 Security – Manages cross-platform security functions, such as security incident response, security monitoring, and vulnerability scanning.
- Governance, Risk, and Compliance (GRC) – Identifies, documents, and advises teams in implementing controls to maintain O365's availability and security commitments to its customers.
- Office Trustworthy Computing (OTwC) – Develops and enforces the Secure Development Lifecycle process for O365 applications and support services.
- Identity Management (also known as Access Control team) – Operates the IDM tool to provide access control automation for all teams (excluding Microsoft Teams).
- Microsoft Information Technology (MSIT) – Provides the access control and authentication mechanism for Microsoft Teams via MyAccess.
- Azure – Provides customer authentication infrastructure including Microsoft Online Directory Services, Microsoft Organization ID, and AAD.

- Microsoft 365 Remote Access – Provides internal users remote access control and authentication to the O365 environment.
- Security Incident Response (SIR) – An internally focused resource that provides detection and analysis as well as containment, eradication and remediation for severe security incidents that may affect the O365 services.

Procedures

O365 adheres to Microsoft Corporation's Security Policy, which is owned by the Information Risk Management Council (IRMC), comprising 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

O365 uses National Institute of Standards and Technology (NIST) standard 800-53 for baseline control procedures, which are documented in the O365 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

O365 customer content is maintained in Azure and SQL server databases, which are hosted on a defined Windows AD domain. 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 O365 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 while running the service, which is not linkable to an individual user or tenant and does not contain 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

O365 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 O365), 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 O365 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 O365, but allowed to access, manage, or process information assets of O365 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.

Office of Legal Compliance — Board of Directors and Senior Leadership

The Office of Legal Compliance (OLC) designs and provides reports to the board of directors on compliance matters. The OLC 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.

OLC/IA/Risk Management — Risk Responsibility

The responsibility for risk is distributed throughout the organization based on each individual group's services. OLC, 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

OLC — 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

O365 uses Microsoft Azure including the Microsoft Datacenter service, which manages datacenters, IaaS, and PaaS supporting services for the O365 applications including hosting of servers, network support, authentication, virtual server hosting and system data storage. Note that O365 considers Azure and Microsoft Datacenters as two separate organizations within this report and are defined as such.

The O365 GRC team is responsible for identifying dependencies of each service and monitoring the subservices implementation of agreed-upon security, availability, processing integrity, and confidentiality controls. Dependencies are documented in Inter-Service Agreements. Monitoring includes, but is not limited to, the review of third-party service auditor reports and discussions with subservice organization management.

A brief overview of the subservice organizations used by Microsoft O365 is below.

Organization	Brief Description
Microsoft Azure	Microsoft Azure's cloud PaaS offerings are used by O365 to host production data and handle logical access and change management controls for O365.
Microsoft Datacenters	Microsoft Datacenter's IaaS offerings are used by O365 to host physical and virtual servers and system data storage. Microsoft Datacenters also handles physical and environmental security controls for O365.

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 O365 controls in place to satisfy the criteria are included as part of "Part A" in Section IV of this report and are an integral part of the description of the system.

Business Planning

The O365 planning process is driven by product updates and releases. Senior management defines the vision and strategy for the overall O365 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 O365 personnel through a strategy memo. The O365 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 O365 Security team, which is responsible for overseeing security issues, system operation, and service availability within the O365 environment. In addition, an O365 GRC risk team has been defined and is responsible for management of security, availability, processing integrity, and confidentiality controls within the O365 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 O365 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

O365 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 O365), 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 for all US based full-time employees and vendors before access is granted to certain eligibilities within each workstream. US Background checks are renewed every two years. Microsoft has rolled out an international screening program, which requires background screening and renewals for all new FTE and vendor personnel in forty-four countries, as permitted by the laws of each country.

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 O365 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 O365, 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 O365 environment is used internally to analyze key processes for system operation.

Customer Commitments and Responsibilities

Externally, O365 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 O365 employees through policies, training, and Office Hours. Office Hours are twice-weekly time slots set aside during which O365 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, O365 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 O365 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

O365 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 Beyond Trust, and Office Substrate Pulse. Incidents may also be reported via email by different O365 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 O365 service infrastructure in the Microsoft O365 blog. In addition, O365 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 – O365

O365 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.

O365 is represented on the Operational Enterprise Risk Management (OERM) Governance Committee by the O365 Risk Management Office. For O365 the risk review is done annually, beginning in August. O365 risk management contacts the O365 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. O365 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 O365 control framework. This framework is managed by the O365 GRC group and is evaluated and updated on an ongoing basis. This evaluation includes input from changes to the overall O365 environment, the regulatory landscape, and results of control assessments.

Implementation of the control activities is the responsibility of each of the O365 application and supporting service teams.

Data Flow Diagrams

Data flow diagrams showing O365 system interactions and dependencies are maintained for each service. On a semi-annual basis, these diagrams are updated by GRC personnel with the input of relevant service teams. This is done to provide up to date O365 system design information to O365 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 operating effectiveness 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 O365 GRC team to substantiate that they are addressed in a timely manner.

Access Management

Microsoft O365 environments use an AD infrastructure for centralized authentication and authorization to their systems and services. There are multiple identity access management tools used by the service teams to manage their respective AD domains.

Identity Access Management

Microsoft O365 owns and manages tools that regulate access to O365 production environments. Most service teams use the IDM access management service to limit access to authorized users. The service, managed by the Access Control team, allows each of the other service teams to manage their respective AD clusters for their respective environment. Several backend processes synchronize with other internal Microsoft tools, such as Microsoft HR department systems, to check that user information (e.g., employment status, manager, cost center, background check information) meets predefined requirements. Users who meet predefined criteria can request access to certain eligibilities, and access is only granted after approval.

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

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 O365 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 O365 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 service 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 in each service teams’ and support teams’ Windows AD domain. 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 O365 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 O365 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 O365 applications regardless of device. The external users' access is managed and configured by the customer.

Customer Lockbox

Customer Lockbox is an access control technology included in O365, designed to provide customer control and transparency over access to customer content hosted in Microsoft datacenters. The service grants Microsoft engineers temporary access to customer content on as-needed basis only as approved by an appropriate tenant authority. The following sections, prefixed with "Customer Lockbox," detail the procedures in place to limit Microsoft access to customer generated content.

Customer Lockbox - Authorization and Notification

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

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

Customer Lockbox - Customer Approval

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

Customer Lockbox - Associated Service Request

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

Customer Lockbox - Office 365 Admin Center

O365 customers can review a history of Customer Lockbox elevation requests within the customer's O365 Admin center. The history includes relevant information for current and past elevation requests, including the date, service request number, duration of elevation, reason for elevation, and requestor. The logs are kept for a reasonable period of time.

Customer Lockbox - Searchable Audit Logs

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

Customer Lockbox - Management Review of Elevations

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

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 hosted within the associated AD domain. The SSL encryption algorithm is Federal Information Processing Standard (FIPS) 140 compliant.

Additionally, access to the O365 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 O365 application and support services. The encryption levels are set by the customer, but each O365 service team has a specified and maintained listing of allowable encryption protocols that the customer may use.

Encryption between Microsoft datacenters

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

Data at Rest (Encryption)

Customer content at rest in the O365 environment is encrypted at rest utilizing full disk encryption or file level encryption. The data is encrypted using 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 has begun rolling out mailbox level encryption. Additionally, teams that store data on Azure Blob storage utilize Azure's built-in encryption at rest.

Data Segregation

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

Service Encryption with Customer Key in Office 365

Microsoft O365 provides customers with two application level encryption options for their data within Exchange and SharePoint service: 1) Service Encryption with Microsoft owned encryption keys, and 2) Service Encryption with customer-owned keys ("Customer Keys").

In the standard Microsoft Service Encryption described above, O365 owns the encryption keys for the customer's Exchange mailboxes and SharePoint sites. Service Encryption with Customer Key ("Customer Key") is an opt-in encryption offering that allows O365 customers to supply and manage their own encryption keys for advanced, self-managed protection. The Customer Key offering is available in both the Exchange Online Worldwide, GCC-M, GCC-H, Department of Defense environment, as well as the SharePoint Online Worldwide environment.

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

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

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

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

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

Microsoft provides additional protections if the customer owned root keys are lost or stolen with an "Availability Key", which provides O365 customers with the capability to recover from the unanticipated loss of root keys. Microsoft will either assist customers through this process or provide customers with instructions on how to recover without assistance from Microsoft.

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

Service Encryption with Customer Key in Office 365 – Termination

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

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

Network Management

Network Problem Management

Microsoft Datacenters' Global Networking Services (GNS) has designated teams (i.e., Problem Management, Network Escalations, and Network Security) to identify and address security alerts and incidents. GNS is responsible for identifying and analyzing potential problems and issues in the Microsoft Office 365 Services networking environment.

Network Configuration Monitoring

Microsoft Datacenters' GNS team has implemented procedural and technical standards for the deployment of network devices. These standards include baseline configurations for network devices, network architecture, and approved protocols and ports. GNS regularly monitors network devices for compliance with technical standards and potentially malicious activity.

Network Change Management

GNS has implemented a formal change management process that requires network changes, including configuration changes, emergency changes, Access Control Lists changes, and new deployments to be documented and authorized prior to implementation. Changes and change approvals are tracked in a ticketing system.

Server/Network Device Remote Access

Microsoft Datacenters provides remote server and network device access to Microsoft Datacenters-managed environments. Access is provided through Microsoft Datacenters-managed Active Directory security groups and follows standard logical access procedures as established by Microsoft Datacenters and GNS.

Server Build-out Process

O365 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 AD 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 one of two processes for server build-out compliance:

- Quality assurance checklist/Automated scan:

  As part of the build-out process, each server is scanned using an automated tool. This scan produces a log file that details if the applicable build-out steps were followed and completed successfully. In addition to this scan, teams follow a manual checklist to ascertain that some steps have been completed in the build-out process, which includes evaluating the automated scan log file.

- 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 the master antimalware server hosted within the service team's AD domain. 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.

Vulnerability and Patch Management

The O365 Security team monitors for known configuration and patching vulnerabilities through automated scans based on Beyond Trust technology. A master server is configured to scan each server within O365 applications and supporting services AD domains to analyze and report known vulnerabilities and patch non-compliance. Each service team reviews the vulnerability scan report from the master server and assesses the criticality of the vulnerabilities and applies patches as applicable.

New vulnerabilities (e.g., those from responsible disclosure programs) are communicated to O365 through the Microsoft Security Response Center. If a patch is developed for the vulnerability, each service team evaluates the relevance of the patch to its environment and applies the patch as applicable.

Security Incident Monitoring

O365 has implemented incident response procedures, which consist of technical mechanisms, organizational infrastructure, and other procedures to detect, respond, and deter security incidents. The O365 incident management technical infrastructure includes monitoring systems for detecting and alerting O365 personnel of security events and incidents. A monitoring agent is installed on each server at the time of server build-out to transfer the security logs to the Security Incident Response (SIR) team, which identifies potential incidents and serves as a central repository for investigations. Incidents posing significant risk to the environment are prioritized for response and mitigation.

Additionally, each service team has on-call personnel covering a 24/7 schedule. If an incident is assigned a high enough severity, applicable contingency plans are invoked. When a contingency plan is invoked, the incident manager on shift works with the O365 Security team to implement the contingency plan.

Service Infrastructure and Support Systems Change Management

Service- and support-related changes follow an established change management process for the O365 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 O365 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, O365 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 O365 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.

O365 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

O365 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, OTwC, 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

O365 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, O365 senior management reviews capacity, availability, and resiliency reports from the above tools, for anomalies and deviations that could impact availability. On a monthly basis, O365 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

Data for customer content, applications and support services is replicated for redundancy and disaster recovery purposes. O365 applications and supporting services are generally replicated from the primary content database to a secondary content database within the same primary datacenter. The primary and secondary databases are then replicated across geographically dispersed datacenters. Generally, the data maintained in the primary content database is replicated and accessible in real time via: (1) the primary database; (2) a secondary replication database located in the same primary datacenter with real time data; (3) a secondary disaster recovery server with real time replicated data in a geographically segregated datacenter; or (4) a server with a few minutes lag replication in a geographically dispersed datacenter.

In addition to content replication and geographical redundancy, O365 customer content data is also subject to a periodic Azure Blob Storage backup process. Customer content is generally subject to three backup types, each with a unique cadence:

- Full Backups – Full backups consist of all customer content data on a server or content database, generally occur on a weekly frequency and are maintained for 30 days.
- Differential Backups – Differential backups occur at a daily frequency and consist of any additional data since the last full backup or differential backup, depending on which was the last to occur.
- Transaction-Log Backups ("TLog") – TLog backups occur every 5 minutes and consist of any additional data added in every 5-minute interval.

As data is accessible for redundancy and disaster recovery purposes for applications and support services through the data replication process described above, data backup is performed on applications containing customer content to meet the SLA requirements.

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

Business Continuity

The majority of O365 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 O365 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 O365 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 O365 environments related to confidentiality.

Processing and Data Integrity

O365 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

O365 monitors its dependencies on third parties through obtaining and evaluating attestation reports when available.

Customer content is retained after termination of O365 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 O365 environments related to confidentiality.

O365 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 in **Section IV** under **Part A**. The testing procedures performed over the related control activities are listed in **Section IV** under **Part B** of this report, "Information Provided by Independent Service Auditor Except for Trust Services Criteria and Control Activities," to reduce the redundancy that would result from listing them in this section and repeating them in **Section IV**. While these controls are listed in **Section IV**, the service organization remains responsible for the representations in the description of controls. These control activities include preventive, detective, and corrective policies and procedures that help O365 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 O365 service. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. O365 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 O365'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 Online Service Terms, Microsoft Product Licensing, 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: O365 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: O365 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: O365 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: O365 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 are communicated in O365's system policies and procedures, system design documentation, and contracts with customers. 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 have been documented on how to carry out specific manual and automated processes required in the operation and development of various O365 services.

Complementary User Entity Control Considerations (CUECs)

Microsoft O365 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 O365. The following list contains controls that O365 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-05: User entities manage anonymous access to SPO and SfB sessions.	CC6.1
CUEC-06: User entities secure the software and hardware used to access O365.	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-09: User entities are responsible for enabling and maintaining email restoration for EXO.	CC9.1, A1.2, A1.3
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 O365 for completeness, accuracy, and timeliness.	PI1.2
CUEC-12: User entities are responsible for managing their data processing within O365 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
CUEC-14: User entities are responsible for managing their data output from O365 for completeness, accuracy, and timeliness.	PI1.4
CUEC-15: When employing Customer Lockbox, user entities are responsible for reviewing Microsoft requests to customer content and approving appropriate requests in a timely manner.	CC6.1

Complementary User Entity Controls	Relevant SOC 2 Control Criteria
CUEC-16: User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for importing or generating their own encryption keys.	CC6.7, C1.1
CUEC-17: User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for restricting access to the Azure Key Vault subscription.	CC6.7, C1.1
CUEC-18: User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for rotating customer managed keys per their compliance policies.	CC6.7, C1.1

Complementary Subservice Organization Controls (CSOCs)

Microsoft's controls related to the O365 system detailed in this report cover only a portion of overall internal control for each user entity of O365. It is not feasible for the control criteria related to O365 to be achieved solely by Microsoft. Therefore, in conjunction with O365's controls, a user entity must take into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as follows.

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant 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 O365. 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, incident, and vulnerability management.	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
Infrastructure as a Service	Microsoft Datacenters	Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities supporting O365, including datacenters. Additionally, Microsoft Datacenters is responsible for maintaining controls over: • environmental threats (including natural disasters and man-made threats) • the protection of network equipment (including firewalls and other devices). • security, incident, and vulnerability management.	CC6.4, CC6.5, CC6.7, CC7.1, CC7.2, CC7.3, CC7.4, CC7.5, CC9.1, A1.2, A1.3, C1.1, PI1.5

Section IV:
Information Provided by Independent Service Auditor, Except for Trust Services Criteria and Control Activities

Section IV:
Information Provided by Independent Service Auditor, Except for Trust Services Criteria and Control Activities

Introduction

This report, including the description of tests of controls and results thereof in this section, is intended solely for the information and use of Microsoft Corporation ("Microsoft"), user entities of Microsoft's system related to related to its Microsoft Office 365, including Office 365 with International Traffic in Arms Regulations (ITAR)[4] Support, online services ("O365"), during some or all of the period October 1, 2019, through September 30, 2020, 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 the service organization; how the service organization's system interacts with user entities, subservice organizations, and other parties; internal control and its limitations; complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria; the applicable trust services criteria; and the risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

- The controls established and specified by Microsoft to achieve the specified trust services criteria.

Also included in this section is the following information provided by Deloitte & Touche LLP:

- A description of the tests performed by Deloitte & Touche LLP to determine whether Microsoft's controls were operating with sufficient effectiveness to achieve specified trust services criteria. Deloitte & Touche LLP determined the nature, timing, and extent of the testing performed.
- The results of Deloitte & Touche LLP's tests of controls.

The examination was conducted in accordance with the criteria as set forth in DC Section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Microsoft's 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, of the American Institute of Certified Public Accountants (AICPA), and the AICPA Statement on Standards for Attestation Engagements No. 18 (SSAE 18) and International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. SSAE 18 is inclusive of the following: (1) AT-C 105, Concepts Common to all Attestation Engagements; and (2) AT-C 205, Examination Engagements. Our testing of Microsoft's controls was restricted to the controls identified by Microsoft to meet the criteria related to security, availability, processing integrity, and confidentiality listed in Section IV of this report and was not extended to controls described in

[4] This report is a description of the "Microsoft Office 365 with ITAR Support system" (O365) as defined in the system description. The inclusion of the ITAR reference in the formal name of the system is not intended to examine or opine on the requirements of the United States International Traffic in Arms Regulations (ITAR).

Section III but not included in Section IV, or to controls that may be in effect at user organizations or subservice organizations.

It is each user's responsibility to evaluate the information included in this report in relation to internal control in place at individual user entities and subservice organizations to obtain an understanding and to assess control risk at the user entities. The controls at user entities, subservice organizations, and Microsoft's controls should be evaluated together. If effective user entity or subservice organizations controls are not in place, Microsoft's controls may not compensate for such weaknesses.

Control Environment Elements

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design, implementation, and operating effectiveness of controls identified by Microsoft, our procedures included tests of the following relevant elements of Microsoft's control environment:

a. Integrity and Ethical Values
b. Microsoft SBC
c. Training and Accountability
d. Commitment to Competence
e. OLC, IA Department, AC
f. Risk Assessment
g. Information and Communication
h. Monitoring

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of Microsoft's activities and operations, inspection of Microsoft's documents and records, and re-performance of the application of Microsoft's controls. The results of these tests were considered in planning the nature, timing, and extent of our testing of the control activities described in this section.

Tests of Operating Effectiveness

Our tests of the controls were designed to cover a representative number of transactions throughout the period from October 1, 2019, through September 30, 2020. In determining the nature, timing, and extent of tests, we considered, (a) the nature and frequency of the controls being tested, (b) the types of available evidential matter, (c) the nature of the trust services criteria to be met, (d) the assessed level of control risk, (e) the expected effectiveness of the test, and (f) the results of our tests of the control environment.

Description of Testing Procedures Performed

Deloitte & Touche LLP performed a variety of tests relating to the controls listed in this section throughout the period from October 1, 2019, through September 30, 2020. Our tests of controls were performed on controls as they existed during the period of October 1, 2019, through September 30, 2020, and were applied to those controls relating to the trust services criteria.

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

Test	Description
Corroborative inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control during the reporting period to evidence application of the specific control activity.

Test	Description
Examination of documentation/inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Reperformance of monitoring activities or manual controls	Obtained documents used in the monitoring activity or manual control activity and independently reperformed the procedures. Compared any exception items identified with those identified by the responsible control owner.

Reliability of Information Produced by the Service Organization

We performed procedures to evaluate whether the information provided by the service organization, which includes (a) information provided by the service organization to the service auditor in response to ad hoc requests from the service auditor (e.g., population lists); (b) information used in the execution of a control (e.g., exception reports or transaction reconciliations); and (c) information prepared for user entities (e.g., user access lists), was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes. Information we utilized as evidence may have included, but was not limited to:

- Standard “out of the box” reports as configured within the system
- Parameter-driven reports generated by Microsoft’s systems
- Custom-developed reports that are not standard to the application such as scripts, report writers, and queries
- Spreadsheets that include relevant information utilized for the performance or testing of a control
- Microsoft prepared analyses, schedules, or other evidence manually prepared and utilized by Microsoft

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

Reporting on Results of Testing

The concept of materiality is not applied when reporting the results of tests of controls for which deviations have been identified because Deloitte & Touche LLP does not have the ability to determine whether a deviation will be relevant to a particular user entity. Consequently, Deloitte & Touche LLP reports all deviations.

Description of Control Activities

The information regarding the tests of operating effectiveness is explained below in two parts:

- **Part A**: Contains the Trust Services Criteria, and the related O365 control activities that cover those criteria.
- **Part B**: Contains the details of the test procedures performed to test the operating effectiveness of the O365 control activities and the results of the testing.

The Security, Availability, Processing Integrity, and Confidentiality Trust Services Criteria and O365 Control Activities in **Part A** and **Part B** are provided by Microsoft.

Note: In Part B, 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-28, CA-42, CA-52, and ELC-05.

Part A: Trust Services Criteria and O365 Control Activities provided by Microsoft

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

CC1.0 – Common Criteria Related to the Control Environment

Criteria	Office 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 Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees through an internal Microsoft site. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Periodically, the OLC releases a 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 –** Office 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. Employees are required to acknowledge agreements to return Microsoft assets upon termination.

Criteria	Office 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 –** Office 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 –** An Office 365 security team has been defined and is responsible for Security issues within the Office 365 environment. Service teams have operations personnel who are responsible for system operation and service availability. **CA-02 –** An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment. **CA-17 –** Office 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	Office 365 Control Activity
CC1.4 – COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objective.	**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 O365. Job descriptions include desired candidate competencies and expected job roles and responsibilities. **CA-07 –** Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees through an internal Microsoft site. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Periodically, the OLC releases a 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 Office 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 Office 365 production assets containing customer content. **CA-17 –** Office 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	Office 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 –** An Office 365 security team has been defined and is responsible for Security issues within the Office 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 O365. Job descriptions include desired candidate competencies and expected job roles and responsibilities. **CA-07 –** Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees through an internal Microsoft site. The SBC reflects Microsoft’s continued commitment to ethical business practices and regulatory compliance. Periodically, the OLC releases a 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 O365 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 O365 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. Employees are required to acknowledge agreements to return Microsoft assets upon termination. **ELC-14 –** Employee and vendor agreements communicate the consequences of violating relevant laws, regulations, provisions, and policies regarding information security.

CC2.0 – Common Criteria Related to Communication and Information

Criteria	Office 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 –** An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 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 –** Semi-annually, the Governance, Risk, and Compliance team updates the data flow diagrams and service offerings of O365 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 Office 365 control framework. **CA-17 –** Office 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 Office 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	Office 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 –** An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment **CA-07 –** Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees through an internal Microsoft site. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Periodically, the OLC releases a 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 Office 365 control framework. **CA-12 –** Office 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 Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes. **CA-26 –** Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked until resolution in an incident tracking system **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-13 –** Microsoft communicates employee and vendor obligations to comply with relevant laws, regulations, provisions, and policies regarding information security through employment and vendor agreements.

Criteria	Office 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 Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees through an internal Microsoft site. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Periodically, the OLC releases a 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 –** Office 365 provides customers and external users self-service with compliance reporting related to Office 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 –** Office 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 Office 365 environment are communicated through the Message Center which is part of the Office 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 –** Office 365 monitors its dependencies on Microsoft Azure through obtaining and evaluating attestation reports when available. **CA-59 –** Customer Lockbox elevation requests are displayed in the tenant Office 365 Admin Center. **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-13 –** Microsoft communicates employee and vendor obligations to comply with relevant laws, regulations, provisions, and policies regarding information security through employment and vendor agreements **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	Office 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 –** An Office 365 security team has been defined and is responsible for Security issues within the Office 365 environment. Service teams have operations personnel who are responsible for system operation and service availability. **CA-02 –** An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 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 –** Office 365 system information regarding the design and operation of its services is available to users online through Microsoft web portals. **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 O365 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 O365 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 Office 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	Office 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-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 the Statement of Work template. 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 Office 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 Office 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 –** Office 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 O365 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 O365 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 Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes.

Criteria	Office 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-27 –** There is a continual process for host vulnerability scanning, reporting, and management review within the Office 365 environment. Individual or centralized service teams apply patches and remediate vulnerabilities, which are verified and reported to management through a common process. Responses are tracked for both compliant and non-compliant hosts to identify any outstanding vulnerabilities that need to be addressed by the service teams. **CA-53 –** Office 365 monitors its dependencies on Microsoft Azure 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-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 BCM charter provides a strategic direction and leadership to all Microsoft Engineering organizations. BCM 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. **CUEC-08 –** User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.

Criteria	Office 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 –** Office 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 O365 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 O365 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 Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes. **CA-53 –** Office 365 monitors its dependencies on Microsoft Azure 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	Office 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 O365 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 O365 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 Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes. **CA-53 –** Office 365 monitors its dependencies on Microsoft Azure 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	Office 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 –** An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment. **CA-05 –** Semi-annually, the Governance, Risk, and Compliance team updates the data flow diagrams and service offerings of O365 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 O365 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 O365 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 Office 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	Office 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 –** Semi-annually, the Governance, Risk, and Compliance team updates the data flow diagrams and service offerings of O365 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 Office 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	Office 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 –** An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment. **CA-11 –** On an annual basis services are updated to reflect changes made to the Office 365 control framework. **CA-17 –** Office 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 O365 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 O365 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 Office 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	Office 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 –** An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment. **CA-11 –** On an annual basis services are updated to reflect changes made to the Office 365 control framework. **CA-17 –** Office 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 O365 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 O365 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 Office 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	Office 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 –** An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment. **CA-07 –** Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees through an internal Microsoft site. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Periodically, the OLC releases a 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 Office 365 control framework. **CA-17 –** Office 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 O365 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 O365 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 Office 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.

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

Criteria	Office 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 Office 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 Office 365 production assets containing customer content. **CA-32 –** Access to shared accounts within the Office 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 O365 production environment is approved by an authorized user. **CA-34 –** Identity of users is authenticated to Office 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, Manager / Cost Center changes, group settings, and certificate rotation. **CA-35.b –** Elevated access within the O365 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 Office 365 Service customer's content is segregated either logically or physically from other Online Services customers' content. **CA-39 –** User groups and access control lists have been established to restrict access to Microsoft Datacenters-managed network devices. **CA-40 –** Access to Microsoft Datacenters-managed network devices is restricted through a limited number of entry points that require authentication over an encrypted connection. **CA-41 –** Access to Microsoft Datacenters-managed network devices requires two-factor authentication or other secure mechanisms. **CA-56 –** Customer tenant administrators are automatically notified when a Customer Lockbox elevation request is initiated to access their content. The tenant administrator must authorize the access elevation request prior to access being granted to the content. **CA-57 –** Customer Lockbox elevation requests require management approval prior to submission to the tenant administrator.

Criteria	Office 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.	**CA-58 –** Customer Lockbox elevation requests to customer content require an associated service request. **CA-59 –** Customer Lockbox elevation requests are displayed in the tenant Office 365 Admin Center. **CA-60 –** The workload where the content is accessed logs the access made by the Microsoft Operator, and the entry can be found in the Audit log search. **CA-61 –** Microsoft management reviews both Customer Lockbox and capacity server elevation logs and investigates any anomalies. All elevations statistics are aggregated, reviewed, and reported to management monthly. **CA-64 –** Only keys noted in the tenant's Data Encryption Policy can be used to access the data maintained in that tenant's service encryption. **CA-65 –** Customer content resides in a specific geographic location. **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 O365. **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-05 –** User entities manage anonymous access to SPO and SfB sessions. **CUEC-06 –** User entities secure the software and hardware used to access O365. **CUEC-15 –** When employing Customer Lockbox, user entities are responsible for reviewing Microsoft requests to customer content and approving appropriate requests in a timely manner.

Criteria	Office 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 Office 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 Office 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 O365 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, Manager / Cost Center changes, group settings, and certificate rotation. CA-35.b – Elevated access within the O365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis. CA-39 – User groups and access control lists have been established to restrict access to Microsoft Datacenters-managed network devices. CA-43 – When users no longer require access or upon termination the user access privileges are revoked in a timely manner. 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 O365. CUEC-01 – User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access.

Criteria	Office 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 Office 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 Office 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 O365 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, Manager / Cost Center changes, group settings, and certificate rotation. **CA-35.b –** Elevated access within the O365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis. **CA-39 –** User groups and access control lists have been established to restrict access to Microsoft Datacenters-managed network devices. **CA-43 –** When users no longer require access or upon termination the user access privileges are revoked in a timely manner. **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 O365. **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. **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 O365.

Criteria	Office 365 Control Activity
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.	**CSOC – Microsoft Datacenters –** Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including data centers, supporting O365. Additionally, Microsoft Datacenters is responsible for maintaining controls for O365 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 O365.
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 Office 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements. **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 O365. **CSOC – Microsoft Datacenters –** Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including data centers, supporting O365. **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	Office 365 Control Activity
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**CA-05 –** Semi-annually, the Governance, Risk, and Compliance team updates the data flow diagrams and service offerings of O365 with the individuals that act as point of contact for each service offering. **CA-32 –** Access to shared accounts within the Office 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 O365 production environment is approved by an authorized user. **CA-34 –** Identity of users is authenticated to Office 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, Manager / Cost Center changes, group settings, and certificate rotation. **CA-35.b –** Elevated access within the O365 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-39 –** User groups and access control lists have been established to restrict access to Microsoft Datacenters-managed network devices. **CA-40 –** Access to Microsoft Datacenters-managed network devices is restricted through a limited number of entry points that require authentication over an encrypted connection. **CA-41 –** Access to Microsoft Datacenters-managed network devices requires two-factor authentication or other secure mechanisms. **CA-56 –** Customer tenant administrators are automatically notified when a Customer Lockbox elevation request is initiated to access their content. The tenant administrator must authorize the access elevation request prior to access being granted to the content. **CA-57 –** Customer Lockbox elevation requests require management approval prior to submission to the tenant administrator. **CA-58 –** Customer Lockbox elevation requests to customer content require an associated service request. **CA-59 –** Customer Lockbox elevation requests are displayed in the tenant Office 365 Admin Center. **CA-60 –** The workload where the content is accessed logs the access made by the Microsoft Operator, and the entry can be found in the Audit log search.

Criteria	Office 365 Control Activity
CC6.6 (continued) – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**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 O365. **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 O365.
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 Office 365 Service customer's content is segregated either logically or physically from other Online Services customers' content. **CA-44 –** Data in motion is encrypted when transmitting data between the customer and the data center and between data centers. **CA-45 –** Antimalware detects and prevents introduction of known vulnerabilities and quarantines infected systems. Antimalware signatures are updated as available. **CA-54 –** Data at rest is encrypted per policy. **CA-55 –** Customer content is retained after termination of Office 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements. **CA-62 –** Customer mailboxes are encrypted per customer's defined encryption policies using keys generated and maintained by the customer. **CA-63 –** When a customer requests a data deletion using the Exchange Customer Key service, the data is no longer accessible by Microsoft or the end user. **CA-64 –** Only keys noted in the tenant's Data Encryption Policy can be used to access the data maintained in that tenant's service encryption.

Criteria	Office 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.	**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 O365. **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. **CUEC-04 –** User entities enforce desired level of encryption for network sessions. **CUEC-06 –** User entities secure the software and hardware used to access O365. **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-16 –** User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for importing or generating their own encryption keys. **CUEC-17 –** User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for restricting access to the Azure Key Vault subscription. **CUEC-18 –** User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for rotating customer managed keys per their compliance policies.

Criteria	Office 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-26 –** Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked until resolution in an incident tracking system. **CA-27 –** There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to insure timely resolution of incidents of non-compliance. **CA-38 –** 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 –** Antimalware detects and prevents introduction of known vulnerabilities and quarantines infected systems. Antimalware 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. **CA-47 –** Adverse security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures. **CA-48 –** Microsoft Datacenters-managed network devices are configured to log and collect security events and are monitored for compliance with established security standards. **CUEC-06 –** User entities secure the software and hardware used to access O365.

CC7.0 – Common Criteria Related to Systems Operations

Criteria	Office 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 –** An Office 365 security team has been defined and is responsible for Security issues within the Office 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-27 –** There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to insure timely resolution of incidents of non-compliance. **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 O365 Security team will track and address the issues to resolution. **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. **CA-38 –** 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 –** Antimalware detects and prevents introduction of known vulnerabilities and quarantines infected systems. Antimalware 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. **CA-47 –** Adverse security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures. **CA-48 –** Microsoft Datacenters-managed network devices are configured to log and collect security events and are monitored for compliance with established security standards. **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 O365 services hosted on the Azure platform.

Criteria	Office 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.	**CSOC – Microsoft Datacenters –** Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including configuration management, incident management, and vulnerability scanning and remediation. **CUEC-06 –** User entities secure the software and hardware used to access O365.

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-26 –** Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked until resolution in an incident tracking system. **CA-27 –** There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to insure timely resolution of incidents of non-compliance. **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 O365 Security team will track and address the issues to resolution. **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. **CA-38 –** 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-47 –** Adverse security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures. **CA-48 –** Microsoft Datacenters-managed network devices are configured to log and collect security events and are monitored for compliance with established security standards. **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 –** Office 365 monitors its dependencies on Microsoft Azure through obtaining and evaluating attestation reports when available. **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 O365 services hosted on the Azure platform. **CSOC – Microsoft Datacenters –** Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including configuration management, incident management, and vulnerability scanning and remediation. **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	Office 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-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-26 –** Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked until resolution in an incident tracking system. **CA-27 –** There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to insure timely resolution of incidents of non-compliance. **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 O365 Security team will track and address the issues to resolution. **CA-38 –** 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-47 –** Adverse security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures. **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 O365 services hosted on the Azure platform. **CSOC – Microsoft Datacenters –** Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including configuration management, incident management, and vulnerability scanning and remediation. **CUEC-08 –** User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.

Criteria	Office 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 –** An Office 365 security team has been defined and is responsible for Security issues within the Office 365 environment. Service teams have operations personnel who are responsible for system operation and service availability. **CA-13 –** Incident response guides are used by Office 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 –** Office 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-26 –** Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked until resolution in an incident tracking system. **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 O365 Security team will track and address the issues to resolution. **CA-47 –** Adverse security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures. **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 O365 services hosted on the Azure platform. **CSOC – Microsoft Datacenters –** Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including configuration management, incident management, and vulnerability scanning and remediation. **CUEC-08 –** User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.

Criteria	Office 365 Control Activity
CC7.5 – The entity identifies, develops, and implements activities to recover from identified security incidents.	**CA-01 –** An Office 365 security team has been defined and is responsible for Security issues within the Office 365 environment. Service teams have operations personnel who are responsible for system operation and service availability. **CA-13 –** Incident response guides are used by Office 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 –** Office 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-26 –** Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked until resolution in an incident tracking system. **CA-27 –** There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to insure timely resolution of incidents of non-compliance. **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 O365 Security team will track and address the issues to resolution. **CA-47 –** Adverse security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures. **CA-48 –** Microsoft Datacenters-managed network devices are configured to log and collect security events and are monitored for compliance with established security standards. **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 BCM charter provides a strategic direction and leadership to all Microsoft Engineering organizations. BCM 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.

Criteria	Office 365 Control Activity
CC7.5 (continued) – The entity identifies, develops, and implements activities to recover from identified security incidents.	**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 O365 services hosted on the Azure platform. **CSOC – Microsoft Datacenters –** Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including configuration management, incident management, and vulnerability scanning and remediation. **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	Office 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 Office 365 control framework. **CA-14 –** Changes and updates to the O365 environment are communicated through the admin Message Center part of the O365 Admin Center. **CA-18 –** Changes and software releases within the Office 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 –** 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.

CC9.0 – Common Criteria Related to Risk Mitigation

Criteria	Office 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 O365 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 O365 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. **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 BCM charter provides a strategic direction and leadership to all Microsoft Engineering organizations. BCM 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. **CSOC – Microsoft Azure –** Microsoft Azure is responsible for maintaining controls over data replication and redundancy to the platform services supporting O365. **CSOC – Microsoft Datacenters –** Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including data centers, supporting O365. Additionally, Microsoft Datacenters is responsible for maintaining controls for O365 that address environmental threats including natural disasters and man-made threats. **CUEC-09 –** User entities are responsible for enabling and maintaining email restoration for EXO.

Criteria	Office 365 Control Activity
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 O365 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 O365 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 –** Office 365 monitors its dependencies on Microsoft Azure through obtaining and evaluating attestation reports when available. **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 the Statement of Work template. Outsourced providers are trained to understand and comply with Microsoft's supplier code of conduct. **ELC-13 –** Microsoft communicates employee and vendor obligations to comply with relevant laws, regulations, provisions, and policies regarding information security through employment and vendor agreements. **ELC-14 –** Employee and vendor agreements communicate the consequences of violating relevant laws, regulations, provisions, and policies regarding information security. **ELC-15 –** Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Office 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. **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	Office 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 O365 Security team will track and address the issues to resolution. 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. CA-31 – Office 365 management reviews capacity and availability on a monthly basis. Any issues with or changes to capacity and availability are tracked to resolution. CA-61 – Microsoft management reviews both Customer Lockbox and capacity server elevation logs and investigates any anomalies. All elevations statistics are aggregated, reviewed, and reported to management monthly.
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 O365 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. CUEC-06 – User entities secure the software and hardware used to access O365. CUEC-09 – User entities are responsible for enabling and maintaining email restoration for EXO. CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including datacenters, supporting O365. Additionally, Microsoft Datacenters is responsible for maintaining controls for O365 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 O365.

Criteria	Office 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. **CUEC-09 –** User entities are responsible for enabling and maintaining email restoration for EXO. **CSOC – Microsoft Datacenters –** Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including datacenters, supporting O365. Additionally, Microsoft Datacenters is responsible for maintaining controls for O365 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 O365.

Additional Criteria for Processing Integrity

Criteria	Office 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 –** An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment. **CA-12 –** Office 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 Office 365 data classification process. **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 O365 for completeness, accuracy, and timeliness.
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 –** An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment. **CA-12 –** Office 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. **CUEC-11 –** User entities are responsible for managing their data inputs, and data uploads to O365 for completeness, accuracy, and timeliness. **CUEC-12 –** User entities are responsible for managing their data processing within O365 for completeness, accuracy, and timeliness.

Criteria	Office 365 Control Activity
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 –** Office 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 –** 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 –** Office 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. **CA-56 –** Customer tenant administrators are automatically notified when a Customer Lockbox elevation request is initiated to access their content. The tenant administrator must authorize the access elevation request prior to access being granted to the content. **CA-57 –** Customer Lockbox elevation requests require management approval prior to submission to the tenant administrator. **CUEC-12 –** User entities are responsible for managing their data processing within O365 for completeness, accuracy, and timeliness.
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 –** Office 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 –** 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 –** Office 365 management reviews capacity and availability on a monthly basis. Any issues with or changes to capacity and availability are tracked to resolution. **CA-56 –** Customer tenant administrators are automatically notified when a Customer Lockbox elevation request is initiated to access their content. The tenant administrator must authorize the access elevation request prior to access being granted to the content. **CA-59 –** Customer Lockbox elevation requests are displayed in the tenant Office 365 Admin Center. **CUEC-14 –** User entities are responsible for managing their data output from O365 for completeness, accuracy, and timeliness.

Criteria	Office 365 Control Activity
PI1.5 – System output is complete, accurate, distributed, and retained to meet the entity's processing integrity commitments and system requirements.	**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 O365 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, Manager / Cost Center changes, group settings, and certificate rotation. **CA-35.b –** Elevated access within the O365 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 Office 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements. **CA-60 –** The workload where the content is accessed logs the access made by the Microsoft Operator, and the entry can be found in the Audit log search. **CA-61 –** Microsoft management reviews both Customer Lockbox and capacity server elevation logs and investigates any anomalies. All elevations statistics are aggregated, reviewed, and reported to management monthly. **CA-65 –** Customer content resides in a specific geographic location. **CSOC – Microsoft Azure –** Microsoft Azure is responsible for maintaining controls over data protection for data at rest and in motion to the platform services supporting O365. **CSOC – Microsoft Datacenters –** Microsoft Datacenters is responsible for maintaining controls over physical data storage, protection, and disposal services supporting O365. **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	Office 365 Control Activity
C1.1 – The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	**CA-40 –** Access to Microsoft Datacenters-managed network devices is restricted through a limited number of entry points that require authentication over an encrypted connection. **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 Office 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements. **CA-62 –** Customer mailboxes are encrypted per customer's defined encryption policies using keys generated and maintained by the customer. **CA-63 –** When a customer requests a data deletion using the Exchange Customer Key service, the data is no longer accessible by Microsoft or the end user. **CA-64 –** Only keys noted in the tenant's Data Encryption Policy can be used to access the data maintained in that tenant's service encryption. **CA-65 –** Customer content resides in a specific geographic location. **CA-66 –** Production data is classified and protected based upon the Office 365 data classification process. **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 O365. **CSOC – Microsoft Datacenters**- Microsoft Datacenters is responsible for maintaining controls over physical data storage, protection, and disposal services supporting O365. **CUEC-04 –** User entities enforce desired level of encryption for network sessions. **CUEC-16 –** User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for importing or generating their own encryption keys. **CUEC-17 –** User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for restricting access to the Azure Key Vault subscription. **CUEC-18 –** User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for rotating customer managed keys per their compliance policies.

Criteria	Office 365 Control Activity
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 Office 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements. **CA-63 –** When a customer requests a data deletion using the Exchange Customer Key service, the data is no longer accessible by Microsoft or the end user. **CA-66 –** Production data is classified and protected based upon the Office 365 data classification process.

Part B: Microsoft O365 Control Activities Provided by Microsoft and Test Results Provided by Deloitte & Touche LLP

Control Activity	Tests Performed	Test Result
CA-01 – An Office 365 security team has been defined and is responsible for Security issues within the Office 365 environment. Service teams have operations personnel who are responsible for system operation and service availability.	• Inquired of Governance, Risk & Compliance process owners to ascertain that a defined O365 Security team has been established and that the team's responsibilities include management of security, availability, confidentiality, and processing integrity issues within the O365 environment. • Obtained and inspected an organizational chart demonstrating the existence of a dedicated O365 Security team. • Obtained meeting minutes and policy documentation to ascertain that responsibilities for O365 Security personnel are defined and include the management of security, system operation, and service availability issues in the O365 environment, as well as the design, development, implementation, and maintenance of security, availability, processing integrity, and confidentiality during SDLC changes.	No Exceptions Noted
CA-02 – An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment.	• Inquired of Governance, Risk & Compliance process owners to ascertain that a defined O365 Governance, Risk, and Compliance team has been established and that the team is responsible for overseeing security, availability, confidentiality, and processing integrity controls within the O365 environment. • Obtained and inspected an organizational chart demonstrating the existence of a dedicated O365 Governance, Risk & Compliance team. • Obtained policy documentation to ascertain that responsibilities for O365 Governance, Risk & Compliance personnel are defined and include the management of O365 security, availability, confidentiality, and processing integrity controls.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
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.	• Inquired of Governance, Risk & Compliance process owners to ascertain that Senior Management considers its commitments and requirements related to security, availability, confidentiality, and processing integrity as part of its major system release planning process. • Obtained and inspected a sample selection of evidence including memorandums and planning meeting records, to ascertain that commitments and requirements for security, availability, confidentiality, and processing integrity were considered and approved by Senior Management, and these commitments and requirements were communicated to relevant personnel as part of the major system release planning process.	No Exceptions Noted
CA-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.	• Inquired of HR process owners to ascertain that performance reviews take place where employee commitments are evaluated by his/her manager on a semi-annual basis. • Obtained and inspected extracts from the Connect tool for a selection of employees to ascertain that they completed a performance evaluation annually. • Obtained and inspected extracts from the Connect tool to ascertain that a sample performance review includes an evaluation of employee performance against their assigned priorities.	No Exceptions Noted
CA-05 – Semi-annually, the Governance, Risk, and Compliance team updates the data flow diagrams and service offerings of O365 with the individuals that act as point of contact for each service offering.	• Inquired of Governance, Risk & Compliance process owners to ascertain that O365 data flow diagrams and service offering point of contacts are reviewed and updated on a semi-annual basis. • Obtained and inspected evidence for a sample of data flow diagram updates to ascertain that the GRC team reviews the service offering data flow diagrams with the point of contacts and that they update the data flow diagrams accordingly.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-06 – The Candidates job descriptions are created and documented for open positions within O365. Job descriptions include desired candidate competencies and expected job roles and responsibilities.	• Inquired of Governance, Risk, & Compliance process owners to ascertain that candidate's job descriptions are created and documented for open positions within O365. • Obtained and inspected a sample job posting to ascertain that the job listing includes desired candidate competencies and expected job roles and responsibilities.	No Exceptions Noted
CA-07 – Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees through an internal Microsoft site. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Periodically, the OLC releases a 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.	• Inquired of HR process owners to ascertain that a defined Standards of Business Conduct policy was established and is communicated to Office 365 personnel through intranet sites and trainings. • Obtained and inspected the Standards of Business Conduct to ascertain that the standards include Microsoft's continued commitment to security, availability, confidentiality, and processing integrity, and also, ethical business practices and regulatory compliance. • Obtained and inspected course completion status for a selection of employees to ascertain that the Standard of Business Conduct training course has been completed.	No Exceptions Noted
CA-08 – The Microsoft Office 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 Office 365 production assets containing customer content.	• Inquired of Governance, Risk & Compliance (GRC) process owners that new and transferred applicable employees and contractors are required to undergo a background check prior to being granted access to the environment. • Obtained and inspected background check data for a selection of Microsoft personnel to ascertain that a background check was performed prior to granting access to the production assets containing customer content.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-09 – Office 365 system information regarding the design and operation of its services is available to users online through Microsoft web portals.	• Inquired of Governance, Risk & Compliance process owners to ascertain that O365 system design and operation information is accessible to employees. • Observed the Microsoft web portals to ascertain that design and operation information for the O365 system is available and accessible to users.	No Exceptions Noted
CA-10 – Office 365 provides customers and external users self-service with compliance reporting related to Office 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.	• Inquired of Governance, Risk, & Compliance process owners to ascertain that customers can obtain the SOC report for O365 through the Service Trust Portal. • Observed the Service Trust Portal to ascertain that the O365 SOC report and its associated CUECs is available to customers.	No Exceptions Noted
CA-11 – On an annual basis services are updated to reflect changes made to the Office 365 control framework.	• Inquired of Governance, Risk & Compliance process owners to ascertain that the O365 control framework is reviewed and updated on an annual basis by service teams. • Obtained and inspected documentation from various ticketing systems to ascertain that service teams reviewed the O365 Control Framework with the point of contacts and updated the framework accordingly.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-12 – Office 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.	• Inquired of Governance, Risk & Compliance process owners to ascertain that O365 communicates its regulatory, security, availability, confidentiality, and processing integrity commitments to customers using SLAs, and that these commitments are also distributed internally. • Obtained and inspected policy and communication documentation to ascertain that SLAs defining regulatory, security, availability, confidentiality, and processing integrity commitments are distributed to O365 customers. • Obtained and inspected policy and communication documentation to ascertain that regulatory, security, availability, confidentiality, and processing integrity requirements are distributed internally through methods including trainings, policies, and Office Hours.	No Exceptions Noted
CA-13 – Incident response guides are used by Office 365 personnel for the handling and reporting of security incidents. These guides are stored on internal SharePoint sites and are updated as needed.	• Inquired of Governance, Risk & Compliance process owners to ascertain that incident response guides, which provide guidance on management and reporting of security incidents, are accessible to O365 personnel on internal SharePoint sites. • Obtained and inspected the O365 incident response guides to ascertain that they are available to personnel on the intranet and outline procedures to be followed for handling and reporting of security incidents.	No Exceptions Noted
CA-14 – Changes and updates to the O365 environment are communicated through the admin Message Center part of the O365 Admin Center.	• Inquired of Governance, Risk & Compliance process owners to ascertain that incidents and changes to the O365 environment are made available to customers using the Customer Portal. • Obtained and inspected newsletters for a sample customer to ascertain that monthly newsletters containing O365 incident and change information are available on the Customer Portal.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-15 – Service impacting incidents, including security incidents, are communicated to the customer through the Service Health Center.	• Inquired of Governance, Risk & Compliance process owners to ascertain that information related to security, availability, confidentiality, and processing integrity issues can be reported and received using the Customer Portal. • Obtained and inspected communication documentation for a sample O365 customer to ascertain that security, availability, confidentiality, and processing integrity information is available on their Customer Portal. • Examined published documentation for O365 service health center to ascertain that security, availability, confidentiality, and processing integrity information is available to all customers.	No Exceptions Noted
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.	• Inquired of Governance, Risk & Compliance process owners to ascertain that customers can report security, availability, confidentiality, and processing integrity incidents by calling the Customer Support Services (CSS) phone number, or by submitting the incident through the Microsoft website. • Obtained and inspected O365 customer service websites and policies to ascertain the existence of a website and phone number through which O365 customers are able to report their security, availability, confidentiality, and processing integrity incidents. • Observed the Admin Center portal and ascertained that there was the ability to submit a support request ticket for customer incidents or questions.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-17 – Office 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.	• Inquired of Governance, Risk & Compliance process owners to ascertain that the Microsoft Security Policy, which defines accountability for implementing security and evaluating security controls, is available on the intranet and adhered to by O365 personnel. • Obtained and inspected the Microsoft Security Policy to ascertain that it is available to personnel on the intranet and defines responsibilities for implementing and overseeing security and related security controls. • Obtained and inspected policy documentation to ascertain that the Microsoft Security Policy is approved by the Information Risk Management Council chair, the Chief Information Security Officer of Microsoft.	No Exceptions Noted
CA-18 – Changes and software releases within the Office 365 environment are documented / tracked and are approved prior to implementation into production.	• Inquired of Change Management control owners that procedures have been established and are followed prior to deploying changes to the production environment. • Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that deployed changes are documented and tracked within a tracking tool. • Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that deployed changes were approved by appropriate stakeholders prior to release.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
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.	• Inquired of Change Management and Logical Security control owners that for the teams using the Developer / Operations model, restrictions are in place to monitor or limit access to implement unapproved changes. • Observed that monitoring is in place for developers with access to the environment. • Obtain and inspected source code and change ticketing systems to ascertain that system configurations and procedures were in place to identify and remediate unapproved changes.	No Exceptions Noted
CA-20 – Emergency changes to the production environment follow an emergency change approval process.	• Inquired of Change Management control owners that deployed emergency changes are approved by identified key stakeholders prior to release into production. • Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that emergency changes were approved by identified key stakeholders.	No Exceptions Noted
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.	• Inquired of Change Management control owners that testing of changes is documented and required for deployment into production. • Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that changes are tested prior to release according to established procedures. • Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that testing was reviewed and approved prior to release according to established procedures.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
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 O365 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 O365 management with ownership assigned out to individual teams and their management.	• Inquired of Governance, Risk & Compliance process owners to ascertain that a risk assessment and management process has been established for O365 to identify risks related to security, availability, confidentiality, and processing integrity, and is performed and approved on an annual basis. • Obtained and inspected the Risk Management process and policy documents for evidence that a process has been established. • Obtained and inspected the Risk Assessment for Fiscal Year 2020 completed by the O365 team for evidence that the assessment had been completed and risks have been identified. • Obtained and inspected the approvals by O365 management associated with the completion of the Risk Assessment performed.	No Exceptions Noted
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.	• Inquired of Governance, Risk & Compliance process owners to ascertain that a process has been established to track and mitigate risks identified as part of Risk Management process. • Obtained and inspected that for a selection of the risks identified a risk mitigation strategy has been established and has been put in place.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
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.	• Inquired of Governance, Risk & Compliance process owners to ascertain that the effectiveness of existing controls are assessed, both internally and externally, on an annual basis. Further ascertained per inquiry that any findings from these control assessments are addressed with corrective action plans and tracked through to timely resolution. • Obtained and inspected assessment and review reports to ascertain that external control effectiveness reviews are performed and selected a sample of findings from those reviews to test that corrective action plans were developed and tracked for the findings. • Obtained and inspected risk assessment and security scanning reports to ascertain that vulnerability scans and internal risk assessments were performed and selected a sample of findings from those assessments to test that the issues were tracked through to resolution.	No Exceptions Noted
CA-25 – Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes.	• Inquired of Governance, Risk & Compliance process owners to ascertain that the O365 control framework is updated as needed to accommodate regulatory, industry, or technology changes. • Obtained and inspected meeting invites and meeting notes demonstrating that the Governance, Risk & Compliance group met with Microsoft regulatory groups, including CELA (Corporate, External, and Legal Affairs), to discuss regulatory, industry, and technology changes. • Obtained and inspected meeting invites and meeting notes to ascertain that service teams reviewed the O365 control framework with the point of contacts and updated the framework accordingly.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-26 – Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked until resolution in an incident tracking system.	• Inquired of Monitoring and Incident management process owners that processes for identifying, reporting, and responding to security incidents have been established. • Obtained and inspected incident documentation for a selection of incidents to ascertain that identified security incidents were documented within an incident tracking system and resolved. • Inquired of Monitoring and Incident management process owners that processes for addressing security incidents have been established and include processes for escalation and review. • Obtained and inspected incident documentation for a selection of incidents to ascertain that security incidents were escalated and reviewed by the appropriate team and required action was taken.	No Exceptions Noted
CA-27 – There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to insure timely resolution of incidents of non-compliance.	• Inquired of Monitoring and Incident management process owners that processes for security vulnerability scanning have been established and outline requirements for addressing identified issues. • Obtained and inspected security scanning reports that vulnerability scans were being performed and completing successfully over the O365 environment. • Obtained and inspected security scanning reports for a selected date to ascertain that scan results were being reviewed and issues noted were being tracked to resolution.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
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 O365 Security team will track and address the issues to resolution.	• Inquired of Operations process owners to ascertain that each workload has on-call personnel established to identify and assist in security, availability, confidentiality, and processing integrity incidents. • Observed and inspected the on-call listing for each workload for evidence that on-call personnel have been established and the on-call personnel covers a 24 hours / 7 days schedule. • Inquired of Monitoring and Incident management process owners that processes for identifying, reporting, and responding to security incidents have been established. • Obtained and inspected incident documentation for a selection of incidents to ascertain that identified high severity security incidents were documented within an incident tracking system and resolved.	No Exceptions Noted
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.	• Inquired of Operations process owners to ascertain that each workload has established a dashboard for monitoring capacity and availability. • Observed and inspected the capacity and availability dashboards for each workload for evidence that capacity and availability metrics are being tracked and displayed to identify service-related issues. • Obtained and inspected an example automated availability alert to ascertain that alerting is in place and incidents are resolved as needed. • Obtained and inspected incident documentation for a selection of incidents to ascertain that capacity and availability incidents were escalated and reviewed by the appropriate team and required action was taken.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-31 – Office 365 management reviews capacity and availability on a monthly basis. Any issues with or changes to capacity and availability are tracked to resolution.	• Inquired of Operations and Governance, Risk & Compliance process owners to ascertain that capacity and availability are reviewed on a monthly basis by O365 management. • Obtained and inspected that for a selection of Monthly Service Review meetings, O365 management reviews capacity and availability issues on a monthly basis.	No Exceptions Noted
CA-32 – Access to shared accounts within the Office 365 environment are restricted to authorized personnel.	• Inquired of Operations and Security process owners to ascertain that shared accounts within the workloads are restricted to authorized personnel. • Obtained and inspected logging and monitoring documentation and security configurations to ascertain that shared user accounts are identified and managed by the workloads to restrict access to authorized personnel.	No Exceptions Noted
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.	• Inquired of Logical Access control owners that processes have been established for requesting and approving access prior to access being granted. • Identified population of users whose access had been modified or granted during the reporting period. • Obtained and inspected access request documentation for a selection of users to ascertain that a request for access was submitted and authorized prior to implementation.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-33.b – Elevated access within the O365 production environment is approved by an authorized user.	• Inquired of Logical Access control owners that processes have been established for requesting and approving access prior to access being granted. • Observed and inspected the system configurations for elevated access within the O365 production environment to ascertain that elevated access is restricted to only approved individuals and is limited based on the established time constraints (for Just in Time Systems). • For Just in Time Systems - Observed for a sample of one user per just in time system that the individual was approved prior to access being elevated, and that the access duration was limited to the requested time. • For Standing Access Systems - Obtained and inspected access request documentation for a selection of users to ascertain that a request for access was submitted and authorized prior to implementation.	M365 Remote Access This control activity could not be tested as there was no related activity during the examination period. All Other Services No Exceptions Noted
CA-34 – Identity of users is authenticated to Office 365 Services. The use of passwords incorporates policy on periodic change and password complexity.	• Inquired of Logical Access control owners that authentication processes and password policies are enforced. • Observed system configuration settings for a selected server for each service to ascertain that authentication polices regarding change intervals and complexity are being enforced.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-35.a – Access to privileged accounts is configured to be revoked automatically based on access expiration settings, including inactivity, Manager / Cost Center changes, group settings, and certificate rotation.	• Inquired of the O365 team that processes have been established for identity access management system configuration to revoke access automatically based on account expiration settings, including inactivity, Manager / Cost Center changes, group settings, and certificate rotation. • Obtained and inspected source code of the system configurations within the identity access management tools to corroborate that account expiration settings, including inactivity, Manager / Cost Center changes, and group settings are configured to remove access. • Obtained and inspected system logs and tracking tickets for selected individuals that expiration settings were enforced, and access was removed based on the configurations within the identity access management system.	No Exceptions Noted
CA-35.b – Elevated access within the O365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis.	• Inquired of the O365 team that processes have been established for reviewing elevated access that is not automatically expired. • Obtained and inspected user access review documentation for selected quarters to ascertain that access was reviewed, and any identified issues were addressed in a timely manner.	SPO Within the Quarter 1 user access review, for one of the twenty-five users selected to validate appropriateness of access granted ascertained that access was not marked for removal and thus the individual was not removed in a timely manner. The individual was removed in the next quarterly review. EOP-IP User access reviews were not performed for the EOP-IP Model D sub-services from Quarter 1 through Quarter 3. All Other Services No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-36 – Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.	• Inquired of Logical Access owners to gain an understanding of how authentication is enforced, and processes established with relation to encrypting communication with the production environment. • Observed authentication to a selected production server to corroborate that two-factor authentication was required. • Obtained and inspected source code configurations and system settings corroborating the encryption settings enforced for accessing the production environment.	No Exceptions Noted
CA-37 – Each Office 365 Service customer's content is segregated either logically or physically from other Online Services customers' content.	• Inquired of security process owners to gain an understanding of the processes that enforce segregation, either physically or logically, of customer content. • Obtained and inspected a sample of physical server configurations and tested user interfaces to ascertain that customer content is segregated.	No Exceptions Noted
CA-38 – Production servers go through a quality assurance review prior to installation in the production environment to confirm the server is configured in compliance with baseline security and operational settings according to the server's intended use.	• Inquired of Server Build-out management process owners that processes have been established to have baseline security and operational settings applied to all new servers deployed to the production environment. • Obtained and inspected system logs, source code configurations, and system change documentation for a selection of new servers to ascertain that baseline builds have been established, approved, and deployed prior to a new server being implemented in production.	M365 Remote Access This control activity could not be tested as there was no related activity during the examination period. All Other Services No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-39 – User groups and access control lists have been established to restrict access to Microsoft Datacenters-managed network devices.	• Inquired of Global Networking Services (GNS) process owners to ascertain that procedures are in place for restricting access to Microsoft Datacenters managed network devices. Inquired that user groups have been created and enforced via the Active Directory. • Obtained and inspected a sample of network devices and inspected their configuration and tested that TACACS+/Radius are used for authentication, authorization of access and that ACLs have been applied.	No Exceptions Noted
CA-40 – Access to Microsoft Datacenters-managed network devices is restricted through a limited number of entry points that require authentication over an encrypted connection.	• Inquired with the GNS process owners to ascertain that access to the network devices in the Microsoft Datacenters environment is restricted through a limited number of entry points which require authentication over an encrypted Remote Desktop connection. • Inspected the GNS Account Management SOP and tested that procedures are established to restrict user access to Microsoft Datacenters-managed network devices in the scope boundary, through a limited number of entry points that require authentication over an encrypted connection. • Selected a sample of Microsoft Datacenters-managed network devices and tested that remote access to network devices involves login to GNS RDG, using domain credentials and Smart card followed by login to internal-facing terminal server using domain credentials and Secure Shell (SSH) has been enforced to access the network device. • Obtained the list of terminal servers and tested that access to network devices is restricted through a limited set of terminal servers. Selected a sample of network devices and inspected their configuration and tested that device access is restricted via above terminal servers.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-41 – A Access to Microsoft Datacenters-managed network devices requires two-factor authentication or other secure mechanisms.	• Inquired of GNS process owners to ascertain that two-factor authentication is enforced while connecting to a network device. • Selected a sample of network devices and observed that login to these network devices required two-factor authentication. • Inspected obtained device configuration files for a selection of network devices to ascertain that they were configured to enforce two-factor authentication through TACACS+ or RADIUS servers.	No Exceptions Noted
CA-43 – When users no longer require access or upon termination the user access privileges are revoked in a timely manner.	• Inquired of security management to gain an understanding of the process for disabling or removing access in a timely manner. • Compared a listing of all terminated/ transferred users within the examination period with active user accounts in O365 environments to ascertain if access for terminated/ transferred employees was revoked. Additionally, compared HR Termination reports to O365 security groups to ascertain that removals of terminated users were executed in a timely manner by comparing the users' termination dates against the date of access revocation.	No Exceptions Noted
CA-44 – Data in motion is encrypted when transmitting data between the customer and the data center and between data centers.	• Inquired of Operations and Security process owners to ascertain that for workloads that transmit customer content, these transmissions are performed using encryption. • Obtained and inspected the encryption settings and certificates that are established over the customer content transmission paths for the applicable workloads. • Obtained and inspected the encryption settings and certificates that are established over the datacenter transmission paths for the applicable workloads.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-45 – Antimalware detects and prevents introduction of known vulnerabilities and quarantines infected systems. Antimalware signatures are updated as available.	• Inquired of Operations and Security process owners to ascertain that Antimalware has been installed, is running, and is up to date within the O365 environment. • Obtained and inspected that for a selection of one server per service team, Antimalware programs have been installed, are running, and are up to date.	No Exceptions Noted
CA-46 – Production releases undergo a security review prior to their release into the production environment per defined criteria, including a code review.	• Inquired of SDL security process owners to ascertain that changes undergo a security review prior to release. Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that a security review was performed prior to release for each build.	EOP-IP Advanced eDiscovery and Data Insights v2.0 sub-services did not conduct static security testing during the testing period. All Other Services No Exceptions Noted
CA-47 – Adverse security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures.	• Inquired of Monitoring and Incident management process owners that processes for identifying, reporting, and responding to security incidents have been established. • Obtained and inspected incident documentation for a selection of incidents to ascertain that identified security incidents were documented within an incident tracking system and resolved. • Inquired of Monitoring and Incident management process owners that processes for addressing adverse security incidents have been established and include processes for escalation and review. • Obtained and inspected incident documentation for a selection of incidents to ascertain that adverse security incidents were escalated and reviewed by the appropriate team and required action was taken.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-48 – Microsoft Datacenters-managed network devices are configured to log and collect security events and are monitored for compliance with established security standards.	• Inquired of Microsoft Datacenters and Online Services Security & Compliance (OSSC) process owners that network devices are configured to log and collect security events and monitored for compliance with established security standards. • Observed that logging of security events is automated through a security log database. Additionally, observed security events from a sample server are logged as they occur in the security log database. • Obtained and inspected system configurations for a sample of servers and ascertained that the servers were configured to log and collect security events and those logs are monitored for compliance and any necessary items are resolved.	No Exceptions Noted
CA-49 – Procedures have been established for local redundant storage and/or other redundancy measures supporting the availability of applications and customer content.	• Inquired of Data Backup and Restoration process owners that processes have been established for data backups and restorations. • Obtained and inspected evidence for a selection of backups and replications to ascertain that data backups and replication were occurring according to defined procedures and alternative data instances were available for restoration or failover.	No Exceptions Noted
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.	• Inquired of Business Continuity process owners to ascertain that failover tests occur on a regular basis. • Obtained and inspected business continuity documentation and failover logs for a selection of failover tests to ascertain that the tests were completed as designed, and that any issues identified were assigned to an appropriate owner and being tracked to resolution.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-51 – Customer content and services are replicated to a geographically separate location.	• Inquired of Data Backup and Restoration process owners to gain an understanding of the process for locating customer content on replicated instances in geographically separate locations. • Obtained and inspected system configurations and depending on the setup of the service, a selection of data sources, to ascertain that replicated instances reside in geographically separate locations.	No Exceptions Noted
CA-53 – Office 365 monitors its dependencies on Microsoft Azure through obtaining and evaluating attestation reports when available.	• Inquired of Governance, Risk & Compliance process owners to ascertain that O365 monitors its dependencies on Microsoft Azure, and their compliance with SLAs / contract obligations. • Obtained and inspected meeting minutes and supporting documentation to ascertain that Audit Reports for each of the dependent Microsoft Azure were obtained and inspected for issues. Any issues identified were followed-up on with the required party. • Obtained and inspected meeting minutes and supporting documentation to ascertain that O365 monitors the dependencies on Microsoft Azure through the scheduled Office Hours meetings.	No Exceptions Noted
CA-54 – Data at rest is encrypted per policy.	• Inquired of Operations and Security process owners to ascertain that for workloads that retain customer content, data at rest has been encrypted. • Obtained and inspected the encryption settings are established over the customer content at rest for the applicable workloads. • Observed for a selected server for each workload that the data stored on the server has been encrypted per policy.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-55 – Customer content is retained after termination of Office 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements.	• Inquired of Operations and Security process owners to ascertain that for workloads that retain customer content, data is removed per customer agreements when the customer's account is deactivated. • Obtained and inspected the system configurations for the applicable workloads that synchronizes customer account status (e.g., Active, Suspended) between Microsoft Azure and the workload. • Obtained and inspected system configurations and customer account status logs to ascertain that each applicable workload is configured to systematically remove customer's data based on their account status and is in line with the agreed upon customer's contract and Service Licensing Agreements.	No Exceptions Noted
CA-56 – Customer tenant administrators are automatically notified when a Customer Lockbox elevation request is initiated to access their content. The tenant administrator must authorize the access elevation request prior to access being granted to the content.	• Inquired of Operations and Security process owners to ascertain that Customer tenant administrators are notified when a Customer Lockbox elevation request is initiated to access their content. • Observed for a selected Customer Lockbox subscriber, that a Lockbox request was submitted and approved by tenant management.	No Exceptions Noted
CA-57 – Customer Lockbox elevation requests require management approval prior to submission to the tenant administrator.	• Inquired of Operations and Security process owners to ascertain that customer Lockbox elevation requests require management approval prior to submission to the tenant administrator. • Obtained and inspected an access elevation log request and noted approvers were assigned to the request. • Obtained and inspected access elevation logs to ascertain that an approval took place before access was granted.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-58 – Customer Lockbox elevation requests to customer content require an associated service request.	• Inquired of Operations and Security process owners to ascertain that Customer Lockbox elevation requests to customer content require an associated service request. • Observed that when a service request number was excluded, the elevation request failed to be processed.	No Exceptions Noted
CA-59 – Customer Lockbox elevation requests are displayed in the tenant Office 365 Admin Center.	• Inquired of Operations and Security process owners to ascertain Customer Lockbox elevation requests are displayed in the tenant Office 365 Admin Center. • Observed the population of Lockbox requests within the Office 365 Dashboard – Admin Center.	No Exceptions Noted
CA-60 – The workload where the content is accessed logs the access made by the Microsoft Operator, and the entry can be found in the Audit log search.	• Inquired of Operations and Security process owners to ascertain that all server that host customer content push audit logs to a repository on a real-time basis. • Observed for a sample elevation log that cmdlet activity was logged accordingly. • Observed for a sample elevation that it can be identified through the Office 365 Dashboard search functionality.	No Exceptions Noted
CA-61 – Microsoft management reviews both Customer Lockbox and capacity server elevation logs and investigates any anomalies. All elevations statistics are aggregated, reviewed, and reported to management monthly.	• Inquired of Operations and Security process owners to ascertain that management reviews both Customer Lockbox and capacity server elevation. • Obtained and inspected a sample of MSR monthly presentations which included elevation statistics and resolutions. Inspected that an approval was required in advance of an elevation request.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-62 – Customer mailboxes are encrypted per customer's defined encryption policies using keys generated and maintained by the customer.	• Inquired with the Customer Key owners to ascertain that each customer is responsible for initiating their service encryption configuration during the Customer Key onboarding process. • Observed a test occurrence of a customer's Customer Key subscription termination process within the production environment to ascertain the customer data was no longer accessible after the tenant's termination of the Customer Key subscription.	No Exceptions Noted
CA-63 – When a customer requests a data deletion using the Exchange Customer Key service, the data is no longer accessible by Microsoft or the end user.	• Inquired with Customer Key owners to ascertain that each customer 'Customer Key' subscription has a unique service encryption identifier and a unique Azure Key Vault to house their root encryption keys. • Obtained and inspected a sample customer 'Customer Key' subscription and ascertained that each of the customer's service encryptions was associated with unique Azure Key Vaults for the respective encryption root keys. • Observed a test occurrence of a failed customer attempt to access an Azure Key Vault that was not associated with their 'Customer Key' service encryption.	No Exceptions Noted
CA-64 – Only keys noted in the tenant's Data Encryption Policy can be used to access the data maintained in that tenant's service encryption.	• Inquired with SharePoint and Exchange service engineers to verify each service account use is logged and monitored. • Observed a user successfully access the Data Encryption Policy associated with the service encryption they were provisioned to and observed that same user's failed attempt to access another service encryption of which the user was not provisioned to.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-65 – Customer content resides in a specific geographic location.	• Inquired with SharePoint and Exchange service engineers to verify that the SharePoint and Exchange services are configured to restrict customer content to defined geographic regions. • Obtained and inspected a sample of geographic regions for both the SharePoint and Exchange services and obtained evidence to ascertain that datacenter and service configurations were setup to restrict customer content to defined regions within each service.	No Exceptions Noted
CA-66 – Production data is classified and protected based upon the Office 365 data classification process.	• Inquired of Governance, Risk & Compliance process owners to ascertain that O365 has an established data classification process. • Obtained and inspected the data classification standard to ascertain that there is a defined O365 data classification process and associated documentation that service teams can use to track and understand the data that they manage, and the associated security, availability, confidentiality, and processing integrity requirements associated with that data.	No Exceptions Noted
ELC-01 – Microsoft's values are accessible to employees via the Values SharePoint site and are updated as necessary by management.	• Inquired of Microsoft management regarding Microsoft's values and the process for updating and making them accessible to employees. • Observed the Values SharePoint site and ascertained that Microsoft's values are defined, updated as needed, and published to employees.	No Exceptions Noted
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.	• Inquired of Microsoft Office of Legal Compliance (OLC) team regarding the mechanisms (email, phone, fax, website) that permit reporting of issues related to Business Conduct. • Accessed each communication mechanism to ascertain that the mechanisms were available and functioning.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
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.	• Inquired of the members of the Audit Committee (AC) to gain an understanding of the Charter and Responsibilities of the Audit Committee and its annual review process. • Obtained and inspected the agenda or meeting minutes to ascertain the annual review of Audit Committee's Charter and Responsibilities Calendar. • Inspected the investor relations website to ascertain that the Audit Committee's Charter and Responsibilities Calendar was published on the website. • Obtained evidence (e.g., meeting invite, meeting minutes) to ascertain quarterly meetings between AC and internal / external auditors.	No Exceptions Noted
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.	• Inquired of Microsoft management to gain an understanding of the Internal Audit Charter and the scope and frequency of assurance activities performed by Internal Audit. • Obtained and inspected the Internal Audit Charter and ascertained that the Charter directs the services of the Internal Audit.	No Exceptions Noted
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.	• Inquired of the members of the Compensation Committee to gain an understanding of the process for planning of executive officer development and corporate succession plans for the CEO and other executive officers. • Obtained and inspected the agenda or meeting minutes to ascertain the annual discussion of the succession plans. • Inspected the Compensation Committee Charter on the investor relations website to ascertain that the Compensation Committee's responsibility included reviewing the succession plan for CEO and other executive officers, on an annual basis.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
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.	• Inquired of the Enterprise Risk Management (ERM) team on the ERM risk assessment process and how risks are identified and managed. • Obtained and inspected the agenda or meeting minutes to ascertain that the ERM risk assessment results are reviewed bi-annually and presented to the Board of Directors for review and consideration of the changes.	No Exceptions Noted
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. Employees are required to acknowledge agreements to return Microsoft assets upon termination.	• Inquired of the Human Resources (HR) team that Non-Disclosure Agreements (NDAs), that include asset protection and return responsibilities, were signed as a part of the onboarding process. • Inspected a sample NDA to ascertain that the agreement included requirements for asset protection, and asset return upon termination of employment. • Obtained and inspected the Reporting Concerns About Misconduct policy, to ascertain if policies around notification of incidents were documented.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
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 BCM charter provides a strategic direction and leadership to all Microsoft Engineering organizations. BCM 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.	• Inquired of Business Continuity process owners to ascertain that Office 365 teams participate in the Enterprise Business Continuity program and abide by the BCM charter • Obtained and inspected that for a selection of failover tests, that the test was completed as designed, and that any issues identified were assigned to an appropriate owner and being tracked to resolution.	No Exceptions Noted
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.	• Inquired of workstream control owners regarding how they evaluate changes to see if they require a risk assessment. • Obtained and inspected risk assessments completed as part of Office Hours to ascertain that for each workstream a risk assessment would be performed for changes based on GRC defined criteria.	No Exceptions Noted
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.	• Inquired of GRC process owners regarding their process for planning and executing audit activities. • Obtained and inspected evidence from the most recent ISO audit of the O365 Germany system to ascertain that an audit plan was defined, corroborate that any access required to perform the audit was approved, and that audit findings were addressed.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
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 the Statement of Work template. Outsourced providers are trained to understand and comply with Microsoft's supplier code of conduct.	• Inquired of Microsoft management regarding the process for: - Citing expectations from outsourced providers to achieve specific deliverables - Training outsourced providers on Microsoft's supplier code of conduct • Obtained and inspected Microsoft's Statement of Work template to ascertain that it cited outsourced providers' role and accountability in achieving specific deliverables. • Inspected the supplier procurement website to ascertain that Microsoft's supplier code of conduct is available and accessible to all outsourced providers. • Observed during the supplier access provisioning process that completion of the supplier code of conduct training is required.	No Exceptions Noted
ELC-13 – Microsoft communicates employee and vendor obligations to comply with relevant laws, regulations, provisions, and policies regarding information security through employment and vendor agreements.	• Inquired of GRC process owners regarding their process for communicating employee and vendor obligations to comply with laws and regulations. • Obtained and inspected the Standards of Business Conduct training transcript to confirm that for all internal employees, obligations are communicated as part of the Standards of Business Conduct training. • Obtained and inspected the Supplier Code of Conduct training transcript to confirm that all external contractors/vendors are informed of their obligations to relevant laws/regulations.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
ELC-14 – Employee and vendor agreements communicate the consequences of violating relevant laws, regulations, provisions, and policies regarding information security.	• Inquired of GRC process owners regarding their process for communicating consequences of violating laws and regulations to employee and vendors. • Obtained and inspected the Standards of Business Conduct training transcript to confirm that for all internal employees, consequences of violating laws and regulations are communicated as part of the Standards of Business Conduct training. • Obtained and inspected the Supplier Code of Conduct training transcript to confirm that all external contractors/vendors are informed of consequences of violating relevant laws/regulations.	No Exceptions Noted
ELC-15 – Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Office 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.	• Inquired of process owners regarding their risk assessment process and how risks are identified and addressed related to external parties (such as customers, contractors and vendors). • Obtained and inspected the latest risk assessment performed by Microsoft Azure management to ascertain that it was complete. • Obtained and inspected the Statement of Work (SOW) template citing external parties' access was restricted authoritatively based on the risk assessment performed.	No Exceptions Noted

Section V:
Supplemental Information Provided by Microsoft

Section V:
Supplemental Information Provided by 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 Office 365 ("O365") 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 O365 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

O365 Domain Name Service (DNS) provides authoritative name resolution for a subset of public-facing domains associated with O365. 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 27001:2013, 27017:2015, and 27018:2014

O365 is compliant with ISO standard 27001:2013 and meets the requirements of ISO 27017:2015 and 27018:2014, published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

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)."

O365 has undergone the ISO 27001 certification process and has been certified by the British Standards Institute (BSI). To view the ISO/IEC 27001:2013 certificates, see the Certificate/Client Directory Search Results page located on the BSI Global website.

NIST 800-53 and FISMA

O365 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.

Management's Response to Exceptions Identified

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

Control Activity & Exception	Management's Response
CA-35.b – Elevated access within the O365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis. SPO Within the Quarter 1 user access review, for one of the twenty-five users selected to validate appropriateness of access granted ascertained that access was not marked for removal and thus the individual was not removed in a timely manner. The individual was removed in the next quarterly review. EOP-IP User access reviews were not performed for the EOP-IP Model D sub-services from Quarter 1 through Quarter 3.	SPO One individual remained in an elevated access group for an extra quarter after change of role in Microsoft. However, it was verified that the individual did not retain the ability to use the elevated access due to complimentary access controls. EOP-IP A review of the access group members showed that all individuals had legitimate business need for access during Q1-Q3. The team has been educated on the importance of access control reviews and has implemented a process for future reviews beginning in Q4 of the audit period of performance.
CA-46 – Production releases undergo a security review prior to their release into the production environment per defined criteria, including a code review. EOP-IP Advanced eDiscovery and Data Insights v2.0 sub-services (Model D) did not conduct static security testing during the testing period.	EOP-IP There were two services, impacted by not having static security code analysis turned on. During the period of performance, the security testing was turned on and validated by the auditors. The service team ran security testing on all the code bases. The service team did not find any indication that these two services had been exploited and the team remediated any issue that was found.

Controls Not Subject to this Examination

Control Activity	Test Result
CA-33.b – Elevated access within the O365 production environment is approved by an authorized user.	M365 Remote Access This control activity could not be tested as there was no related activity during the examination period. All Other Services No Exceptions Noted
CA-38 – 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.	M365 Remote Access This control activity could not be tested as there was no related activity during the examination period. All Other Services No Exceptions Noted