Office 365

Mapping of Cloud Security Alliance Cloud Control Matrix

Published: December 15, 2015

Document type: Public
Document stage: Published
Feedback: CXP Risk Assurance Documentation – cxprad@microsoft.com

Table of Contents

Introduction 3

ISO Certifications for the Office 365 Services Stack 4

Using this Document 4

Audit Assurance and Compliance: Controls AAC-01 through AAC-03 5

Application and Interface Security: Controls AIS-01 through AIS-04 6

Business Continuity Management and Operational Resilience: Controls BCR-01 through BCR-11 7

Change Control and Configuration Management: Controls CCC-01 through CCC-05 10

Datacenter Security: Controls DCS-01 through DCS-09 12

Data Security and Information Lifecycle Management: Controls DSI-01 through DSI-07 14

Encryption and Key Management: Controls EKM-01 through EKM-04 16

Governance and Risk Management: Controls GRM-01 through GRM-11 18

Human Resources: Controls HRS-01 through HRS-11 21

Identity and Access Management: Controls IAM-01 through IAM-13 23

Interoperability and Portability: Controls IPY-01 through IPY-05 27

Infrastructure and Virtualization Security: Controls IVS-01 through IVS-13 28

Mobile Security: Controls MOS-01 through MOS-20 31

Security Incident Management, E-discovery, and Cloud Forensics: Controls SEF-01 through SEF-05 33

Supply Chain Management, Transparency and Accountability: Controls STA-01 through STA-09 34

Threat and Vulnerability Management: Controls TVM-01 through TVM-03 37

Document type: Public
Document stage: Published
Feedback: CXP Risk Assurance Documentation – cxprad@microsoft.com

Introduction

Office 365 provides a set of productivity applications that bring together online versions of our email and collaboration software with our familiar Microsoft Office applications in the cloud. Office 365 is developed and managed by the Office 365 Engineering and Operations team, which uses a limited set of Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) services provided by Microsoft Azure (Azure) and Microsoft's Cloud Infrastructure and Operations team (MCIO).

Office 365 applications run on a cloud infrastructure and are accessible from various client devices. While customers remain in control of their data and have control over some feature and implementation settings, Microsoft manages and controls the underlying cloud infrastructure, networks, servers, operating systems, storage, and the individual configurations thereof. The Office 365 stack, including the portion that is customer-managed, is illustrated below:

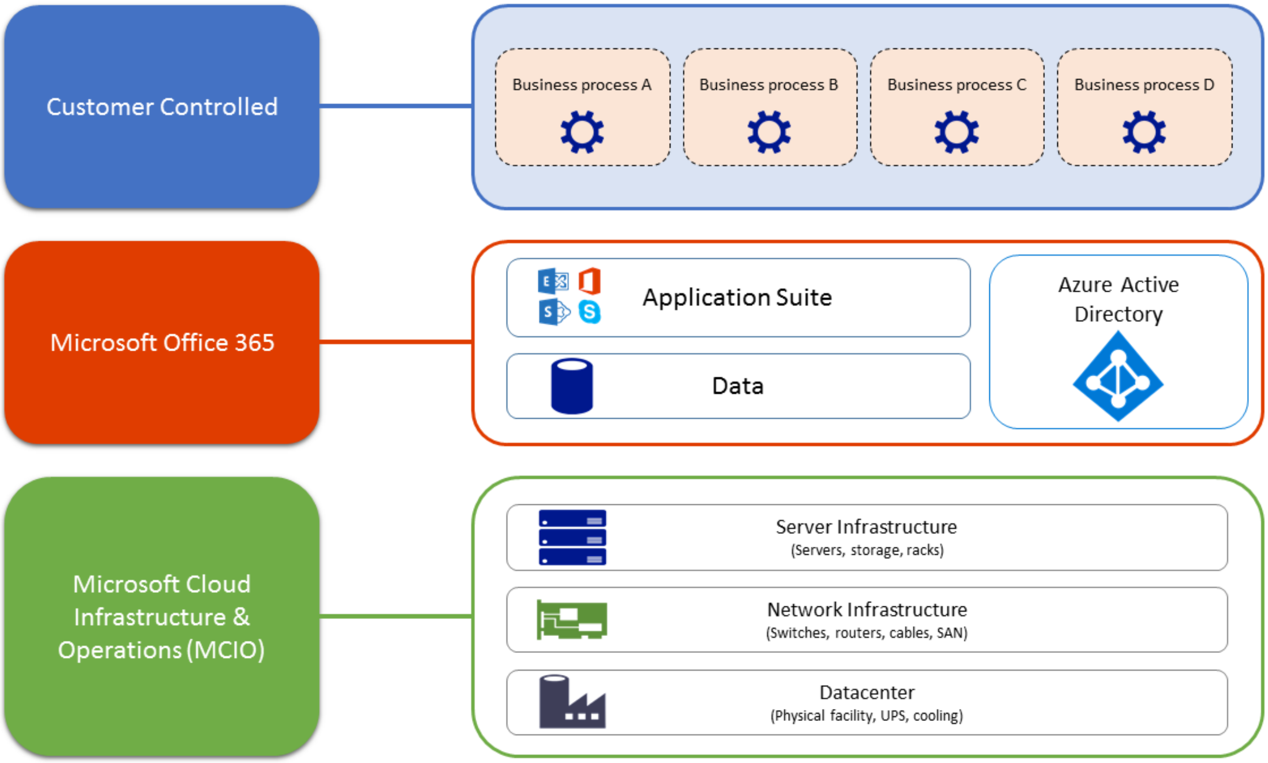

Figure 1 - Customer controlled and Microsoft operated portions of Office 365

Document type: Public
Document stage: Published
Feedback: CXP Risk Assurance Documentation – cxprad@microsoft.com

ISO Certifications for the Office 365 Services Stack

Office 365 and the infrastructure it relies on, which includes Azure and MCIO-managed physical environments, employ security frameworks that span multiple standards, including the ISO 27000 family of standards, guidelines published by the National Institute of Standards and Technology (NIST) like NIST 800-53, and others. Our security framework enables customers to evaluate how Microsoft meets or exceeds its security standards and implementation guidelines. Microsoft's Information Security Policy also aligns with ISO 27002, augmented with requirements specific to Office 365.[1]

A review of the ISO 27001 and ISO 27002 publicly available standards is also recommended. ISO standards are available at the International Organization for Standardization web site. We also recommend that you:

- Visit the independent auditor (BSI) attestation of the Office 365 ISO 27001 Certification
- Visit the independent auditor (BSI) attestation of the Microsoft Azure ISO 27001 Certification
- Visit the independent auditor (BSI) attestation of the Microsoft Cloud Infrastructure and Operations (MCIO) ISO 27001 Certification

In addition, you can download several ISO audit reports from Microsoft's Service Trust Portal (STP), which is available to all Office 365 tenants (including trial subscribers).

Using this Document

In this document, Microsoft provides a detailed overview of how Office 365 maps to the security, privacy, compliance, and risk management controls defined in version 3.0.1-11-24-2015 of the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM). The CSA is a not-for-profit, member-driven organization of leading industry practitioners focused on helping customers make the right decisions when moving to the cloud. The CCM provides a listing of security and privacy controls across 16 domains.

On the following pages, Office 365 security practices are mapped to the control guidance provided by the CCM. The first two columns (CCM Control Domain and ID and CCM v3.0.1 Control Specification) consist of content directly from the CCM identifying relevant controls. The third column (Office 365 Response) consists of short explanations of how Office 365 controls satisfy the CSA recommendations.
The CCM responses included in this document are in alignment with our ISO 27001, 27018 and SOC attestations and scoped to the following Office 365 services that are hosted in Microsoft datacenters:

- Exchange Online
- Exchange Online Protection
- SharePoint Online, including OneDrive for Business
- Skype for Business
- Office Online
- Office Services Infrastructure
- Suite User Experience
- Domain Name Service
- Security Workload Environment

[1] ISO 27002 is not a certification but provides a suggested set of suitable controls for an Information Security Management System (ISMS).

Document type: Public
Document stage: Published
Feedback: CXP Risk Assurance Documentation – cxprad@microsoft.com

Audit Assurance and Compliance: Controls AAC-01 through AAC-03

(Go to Table of Contents)

CCM Control Domain and ID	**CCM v3.0.1 Control Specification**	**Office 365 Response**
Audit Assurance & Compliance *Audit Planning* AAC-01	*Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.*	Office 365 independent audit reports and certifications are shared with customers in the format native to the type of audit. These certifications and attestations accurately represent how Office 365 obtains and meets its security and compliance objectives and serve as a practical mechanism to validate the Office 365 security and compliance promises for customers.
Audit Assurance & Compliance *Independent Audits* AAC-02	*Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.*	SOC, ISO 27001 certifications, and other audit reports for Office 365 can be found at the Office 365 and Microsoft Online Services Security, Audits and Certifications page, and the website of our external ISO auditor, the BSI Group. Applicable audits of Office 365 are carried out at least annually by certified independent assessors, including SOC 1/2, ISO 27001, ISO 27018, and FedRAMP.
Audit Assurance & Compliance *Information System Regulatory Mapping* AAC-03	*Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.*	Office 365 has designed and implemented an Information Security Management System (ISMS) framework that addresses industry best-practices for information security and privacy. The ISMS has been documented and communicated in a customer-facing Information Security Policy, which is available for download from the STP. Office 365 performs annual ISMS reviews, the results of which are reviewed by security and compliance management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions. Office 365 has implemented a common controls framework which maps and aligns control domains and activities across services, requirements, and operations for each audit and certification. This mechanism is regularly maintained and updated with new controls when standards are incorporated into the Office 365 control framework.

Application and Interface Security: Controls AIS-01 through AIS-04

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Application & Interface Security *Application Security* AIS-01	*Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.*	Office 365 ensures application security through a process of continuous security improvement with the Microsoft Security Development Lifecycle (SDL) using both Prevent Breach and Assume Breach security postures. Prevent breach works through the use of ongoing threat modeling, code review and security testing; Assume breach employs Red Team versus Blue Team exercises, live site penetration testing and centralized security logging and monitoring to identify and address potential gaps, test security response plans, reduce exposure to attack and reduce access from a compromised system, periodic post-breach assessment and clean state. Office 365 validates services using third party penetration testing based upon the Open Web Application Security Project (OWASP) top ten and Council of Recognized Ethical Security Testers (CREST)-certified testers. The outputs of testing are tracked through the risk register.
Application & Interface Security *Customer Access Requirements* AIS-02	*Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.*	The Office 365 approach to customer access and trust principles is defined on the Office 365 Trust Center. The principles include built-in security, privacy by design, continuous compliance, and transparent operations. Before using Office 365 services, customers are required to review and agree with the acceptable use of data and the Office 365 service agreement, as well as security and privacy requirements, which are defined in the Microsoft Online Services Use Rights, Microsoft Online Subscription Agreement, Microsoft Office 365 Platform Privacy Statement and Technical Overview of the Security Features in Microsoft Office 365 Platform. To help customers comply with their own requirements, Office 365 builds services with common privacy and security requirements in mind. Office 365 is kept up to date with the ever evolving industry standards and regulations. The service is verified to meet requirements specified in ISO 27001, ISO 27018, HIPAA, FedRAMP and others. The data processing agreement details privacy, security, and handling of customer data, which helps comply with local regulations. Microsoft was the first major cloud service provider to make contractual privacy commitments (as well as to incorporate the best practices encompassed by ISO 27018) that help assure the privacy protections built into in-scope Office 365 services are strong.
Application & Interface Security *Data Integrity* AIS-03	*Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.*	Office 365 defines acceptable standards to ensure that data inputs to application systems are accurate and within the expected range of values. Where appropriate, data inputs are sanitized or otherwise rendered safe before being inputted to an application system. Microsoft developers follow the Microsoft SDL methodology which includes specific requirements for data input and output validation checks. Additional information can be found at the Microsoft Security Development Lifecycle website. Internal processing controls are implemented within the Office 365 environment in order to limit the risks of processing errors. Internal processing controls exist in applications, as well as in the processing environment. Examples of internal processing controls include, but are not limited to, the use of hash totals, and checksums.
Application & Interface Security *Data Security / Integrity* AIS-04	*Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alteration, or destruction.*	Microsoft maintains and regularly updates the Information Security Policy which defines Microsoft policies. The policies address the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365. The Information Security Policy contains policies that must be met in the delivery and operation of Office 365. Standards and Procedures to facilitate execution of these policies are documented in the Office 365 control framework. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks.

Business Continuity Management and Operational Resilience: Controls BCR-01 through BCR-11

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
BCR-01: Business Continuity Management & Operational Resilience - *Business Continuity Planning*	*A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements.* *Requirements for business continuity plans include the following:* • *Defined purpose and scope, aligned with relevant dependencies* • *Accessible to and understood by those who will use them* • *Owned by a named person(s) who is responsible for their review, update, and approval* • *Defined lines of communication, roles, and responsibilities* • *Detailed recovery procedures, manual work-around, and reference information* • *Method for plan invocation*	Management has established roles and responsibilities to oversee implementation of the Information Security Policy and operational continuity across Office 365. Office 365 management is responsible for overseeing security and continuity practices within their respective teams (including third parties), and facilitating compliance with security policies, processes and standards. An Enterprise Business Continuity Management (EBCM) framework has been established for Microsoft and applied to individual business units including Office 365. The designated Office 365 Business Continuity Program Office (BCPO) works with Office 365 management to identify critical processes and assess risks. The Office 365 BCPO provides guidance to the Office 365 teams on EBCM framework and BCM roadmap, which includes the following components: • Governance • Impact Tolerance • Business Impact Analysis • Dependencies Analysis (Non-Technical and Technical) • Strategies • Planning • Testing • Training and Awareness
Business Continuity Management & Operational Resilience *Business Continuity Testing* BCR-02	*Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.*	Business Continuity Plans (BCPs) are documented and reviewed at least annually. The BCPs provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). The Business Continuity team in coordination with the Office 365 service teams conduct testing of the business continuity and disaster recovery plans at least annually. Testing ensures that each loss scenario is tested at least annually. Issues identified during testing are noted and managed to resolution by the Office 365 service team in coordination with the Business Continuity team.
Business Continuity Management & Operational Resilience *Datacenter Utilities / Environmental Conditions* BCR-03	*Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.*	Office 365 operates in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services. Each facility is designed to run all day, every day, and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.
Business Continuity Management & Operational Resilience *Documentation* BCR-04	*Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following:* • *Configuring, installing, and operating the information system* • *Effectively using the system's security features*	Extensive documentation, including standard operating procedures, server baselines and hardening guides, network diagrams, and system build-out documentation is maintained in a secure internal site and made available to authorized personnel as needed.
Business Continuity Management & Operational *Resilience*	*Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind,*	Office 365 operates in geographically distributed Microsoft facilities, in some cases sharing space and utilities with other Microsoft Online Services (paired datacenters are located at least 300 miles apart in order to provide failover in the event of a large-scale regional disaster). Each facility is designed to run all day, every day, and employs various measures to help protect operations from power failure, physical

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Environmental Risks BCR-05	*earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.*	intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.
Business Continuity Management & Operational Resilience *Equipment Location* BCR-06	*To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.*	Microsoft datacenter site selection is performed using a number of criteria, including mitigation of environmental risks. In areas where there exists a higher probability of earthquakes, seismic bracing of the facility is employed. Environmental controls have been implemented to protect systems inside the facility, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.
Business Continuity Management & Operational Resilience *Equipment Maintenance* BCR-07	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.*	Office 365 has established alternate storage sites to permit the storage and recovery of Office 365 backup information. All alternate sites are active sites leveraging near real-time data replication. Each alternate site is redundant and managed by Microsoft in accordance with the recovery time objectives established in the Business Continuity Plans. Additionally, Microsoft provides alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services. Microsoft manages a fiber network where redundant communication links are established following disparate paths through the Microsoft fiber network. This is a continuously operational solution. These redundant links are found in all Microsoft datacenters in which Office 365 operates.
Business Continuity Management & Operational Resilience *Equipment Power Failures* BCR-08	*Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific Business Impact Assessment*	Office 365 has established alternate storage sites to permit the storage and recovery of Office 365 backup information. All alternate sites are active sites leveraging near real-time data replication. Each alternate site is redundant and managed by Microsoft in accordance with the recovery time objectives established in the Business Continuity Plans. Microsoft datacenters have dedicated uninterruptible power supplies (UPS) and emergency power support, which may include generators. Regular maintenance and testing is conducted for both the UPS and generators, and datacenters have made arrangements for emergency fuel delivery. Microsoft datacenters also have a dedicated Facility Operations Center to monitor the power systems, including critical electrical components – generators, transfer switch, main switchgear, power management module and uninterruptible power supply equipment.
Business Continuity Management & Operational Resilience *Impact Analysis* BCR-09	*There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following:* • *Identify critical products and services* • *Identify all dependencies, including processes, applications, business partners, and third party service providers* • *Understand threats to critical products and services* • *Determine impacts resulting from planned or unplanned disruptions and how these vary over time* • *Establish the maximum tolerable period for disruption* • *Establish priorities for recovery* • *Establish recovery time objectives for resumption of critical products and*	Office 365 conducts a risk assessment to identify and assess continuity risks related to Office 365 services. The Business Impact Analysis is carried out and impacts are assessed for critical services based on revenue, reputational, and operational considerations. Business Impact Assessment, Dependency Analysis and Risk Assessments are performed and updated at least annually.

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
	services within their maximum tolerable period of disruption • *Estimate the resources required for resumption*	
Business Continuity Management & Operational Resilience *Policy* BCR-10	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.*	Office 365 has developed a Business Continuity and Disaster Recovery Standard Operating Procedure and documentation that include the defined information security and availability requirements. Office 365 trains personnel in contingency roles and responsibilities through their Office 365 Business Continuity Management Training and Awareness program within 10 days of assuming a contingency role or responsibility. Contingency training will also be conducted as needed when required by information system changes. Refresher training is provided annually. For general information about cloud operations and reliability in Microsoft datacenters, please visit the Microsoft Datacenters page.
Business Continuity Management & Operational Resilience *Retention Policy* BCR-11	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.*	Data retention policies and procedures are defined and maintained in accordance to regulatory, statutory, contractual, and business requirements. If service engineers have questions regarding the retention policies, the Office 365 Compliance team holds regular 'office hours' when engineers can request clarifications as needed. The Office 365 backup and redundancy program undergoes an annual review by independent auditors.

Change Control and Configuration Management: Controls CCC-01 through CCC-05

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Change Control & Configuration Management *New Development / Acquisition* CCC-01	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.*	Office 365 follows NIST guidance regarding security considerations in software development in that information security must be integrated into the SDL from system inception. Continual integration of security practices in the Microsoft SDL enables early identification and mitigation of security vulnerabilities and misconfigurations, awareness of potential software coding challenges caused by required security controls, identification of shared security services, reuse of security best practices tools which improve security posture through proven methods and techniques, and enforces the already comprehensive Microsoft risk management program. Office 365 has established software development and release management processes to control implementation of major changes including: • The identification and documentation of the planned change. • Identification of business goals, priorities and scenarios during product planning. • Specification of feature/component design. • Operational readiness review. • Testing, authorization and change management based on entry/exit criteria.
Change Control & Configuration Management *Outsourced Development* CCC-02	*External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g. ITIL service management processes).*	Office 365 business partners and third-party contractors are required to follow the same established software development and release management processes, including SDL and Operational Security Assurance guidelines, to control implementation of major changes as Office 365 software developers.
Change Control & Configuration Management *Quality Testing* CCC-03	*Organization shall follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.*	Office 365 has developed formal standard operating procedures (SOPs) governing the change management process. These SOPs cover both software development and hardware change and release management, and are consistent with established regulatory guidelines including ISO 27001, SOC 1/SOC 2, NIST 800-53, and others. Microsoft also uses Operational Security Assurance (OSA), a framework that incorporates the knowledge gained through a variety of capabilities that are unique to Microsoft. OSA combines this knowledge with the experience of running hundreds of thousands of servers in datacenters around the world. Microsoft uses OSA to minimize risk by ensuring that ongoing operational activities follow rigorous security guidelines and by validating that guidelines are being followed effectively. The three key processes of OSA are: • Ensuring that OSA inputs (such as organizational learning, threat intelligence, and security technologies) are up-to-date and relevant. • Developing and applying centralized review processes to consolidate requirements to establish the OSA baseline requirements. • Engaging and implementing the new requirements and baselines. Download additional information about how Office 365 uses OSA for change and configuration management here. Critical security review and approval checkpoints are included during the system development life cycle. Business, operational, and technical risks are identified and the areas covered include compliance, security, privacy, and service continuity. As an early pioneer for integrated security development, the SDL is at the core of Office 365, and is a detailed, robust practice that Microsoft has developed over many years. It covers patches, updates, and threat mitigation.

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
		Part of the SDL has been built upon investments in Microsoft Trustworthy Computing. Office 365 has multiple patch management release cycles and engagement models that allow new threats to be quickly mitigated.
Change Control & Configuration Management *Unauthorized Software Installations* CCC-04	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	Changes to production environments go through the Change Management process described in CCC-01 and CCC-03. This process also requires that: • Pre-screened admin requests from Microsoft corporate networks are approved. • That role based access controls are enforced. • Privileges issued grant the least privilege required to complete tasks. • Access requests are logged and audited. Office 365 restricts access to the production environment to approved members of specific security groups. By default, developers and integrators do not have permissions to change hardware, software, or firmware in production. Such permissions can be granted for a short time as needed through just-in-time access elevation. Authorization to elevate access to take such actions is always preapproved before access is granted.
Change Control & Configuration Management *Production Changes* CCC-05	*Policies and procedures shall be established for managing the risks associated with applying changes to:* • *business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations* • *infrastructure network and systems components* *Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.*	Software releases and configuration changes to the Office 365 platform are tested based on established criteria prior to production implementation, and procedures have been established to evaluate and implement Microsoft released patches to Office 365 infrastructure. Customers have access to third party audit reports and certifications that encompass the controls relevant to change management. The reports can be accessed via the STP. Customers also receive their roles, rights and responsibilities in the Office 365 Terms and Conditions.

Document type: Public
Document stage: Published
Feedback: CXP Risk Assurance Documentation – cxprad@microsoft.com

Datacenter Security: Controls DCS-01 through DCS-09

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Datacenter Security *Asset Management* DCS-01	*Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.*	Office 365 has developed, documented, and maintains an asset inventory in a centralized asset reporting database. Asset classifications and attributes are collected defining the minimum data points to determine asset ownership, location, classification, and protection level. Service teams ensure that assets are inventoried monthly, classification and ownership are validated, and associated information is current and accurate. Comparisons are made with scan data to ensure both the reported inventory and the scans accurately reflect the environment. Patching and vulnerability scans are performed on all subnets allocated Office 365, so if an asset has been added to the network without being added to inventory, it will be detected and investigated.
Datacenter Security *Controlled Access Points* DCS-02	*Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.*	Microsoft datacenters receive SOC attestation and are ISO 27001 certified. Microsoft datacenters are located in non-descript buildings that are physically managed, and monitored at all times to protect data and services from unauthorized access as well as environmental threats. Datacenters are surrounded by a fence with access restricted through badge controlled gates. Pre-approved deliveries are received in a secure loading bay and are monitored by authorized personnel. Loading bays are physically isolated from information processing facilities. CCTV is used to monitor physical access to datacenters and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities.
Datacenter Security *Equipment Identification* DCS-03	*Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.*	Microsoft datacenters are operated by the Microsoft Cloud Infrastructure and Operations (MCIO) team, which maintains a current, documented and audited inventory of equipment and network components for which it is responsible. MCIO employs automated mechanisms to detect discrepancies in device configuration by comparing them against the defined policies. MCIO turns off unused ports by default to prevent unauthorized access.
Datacenter Security *Off-Site Authorization* DCS-04	*Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.*	Microsoft asset and data protection procedures provide prescriptive guidance around the protection of logical and physical data and include instructions addressing relocation. Customers control where their data is stored while using Office 365 services during provisioning of their tenant. Details are included in the data maps in the Trust Center. Office 365 does not store backups offsite.
Datacenter Security *Off-Site Equipment* DCS-05	*Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.*	Office 365 follows NIST 800-88 Guidelines for Media Sanitization, which addresses the principal concern of ensuring that data is not unintentionally released. These guidelines encompass both electronic and physical sanitization.
Datacenter Security *Policy* DCS-06	*Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.*	The Information Security policy defines and establishes controls for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information. Access to media storage areas is restricted and audited. Access to Microsoft buildings is controlled through the use of smart cards for Microsoft offices and biometrics for entry into Datacenters. Front desk personnel are required to positively identify full-time employees (FTEs) or authorized contractors. Authorized contractors without ID cards must show government issued IDs for entrance. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. Guests are required to wear guest badges and be escorted by authorized Microsoft personnel.

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Datacenter Security - *Secure Area Authorization* DCS-07	*Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.*	Datacenter entrances are guarded at all times by security personnel and access is controlled through security personnel, authorized badges, biometrics, and locked doors and CCTV monitoring.
Datacenter Security *Unauthorized Persons Entry* DCS-08	*Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.*	Office 365 employees and contractors must have a business need to enter a Microsoft datacenter and have received prior approval by Microsoft personnel. Doors between areas of differing security require authorized badge access, are monitored through logs and cameras, and audited on a regular basis. Failure to abide by the Microsoft Datacenter security policies is grounds for instant dismissal of the employee.
Datacenter Security *User Access* DCS-09	*Physical access to information assets and functions by users and support personnel shall be restricted.*	Access to Microsoft buildings is controlled through the use of smart cards for Microsoft offices and biometrics for entry into Datacenters. Front desk personnel are required to positively identify FTEs or authorized contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. Guests must be escorted by authorized Microsoft personnel when within the datacenter.

Data Security and Information Lifecycle Management: Controls DSI-01 through DSI-07

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Data Security & Information Lifecycle Management *Classification* DSI-01	*Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.*	Office 365 classifies data according to the Office 365 data classification scheme and applies security and privacy controls associated with the data classification. Office 365 treats data created by customers (SharePoint documents, email messages, etc.) as 'customer data' which, along with access control data, is subject to the most rigorous of all security and privacy controls.
Data Security & Information Lifecycle Management *Data Inventory / Flows* DSI-02	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.*	Office 365 has documented and maintains a data flow diagram which accounts for all system connections, the ports and protocols those connections use to communicate, and the classification of data flowing through the connections. The data flow diagram documents inner-system connections and also documents connections with 3rd parties. The Office 365 Security Policy requires that this documentation is reviewed and updated regularly.
Data Security & Information Lifecycle Management *eCommerce Transactions* DSI-03	*Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.*	Office 365 does not provide e-commerce solutions. Customer data will be used only to provide Office 365 services to the customer. This can include troubleshooting aimed at preventing, detecting, and repairing problems affecting the operation of the services and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). More information on the commitments that Microsoft has made regarding the use of customer data can be found in the Office 365 Trust Center.
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy* DSI-04	*Policies and procedures shall be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.*	Office 365 classifies data according to the Office 365 data classification scheme and applies security and privacy controls associated with the data classification. Office 365 treats data created by customers (SharePoint documents, email messages, etc.) as 'customer data' which, along with access control data, is subject to the most rigorous of all security and privacy controls.
Data Security & Information Lifecycle Management *Non-Production Data* DSI-05	*Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.*	Microsoft does not use customer data in non-production environments. In addition, Office 365 is specifically designed to prevent the possibility of production data being moved or replicated outside of the Office 365 environment. These controls include: • Physical and logical network boundaries with strictly enforced change control policies. • Segregation of duties requiring a business need to access an environment. • Highly restricted physical and logical access to the cloud environment. • Strict controls based on SDL and OSA that define coding practices, quality testing and code promotion. • Ongoing security, privacy and secure coding practices awareness and training. • Continuous logging and audit of system access. • Regular compliance audits to ensure control effectiveness.

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Data Security & Information Lifecycle Management *Ownership / Stewardship* DSI-06	*All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.*	Office 365 assets are classified in accordance with the Office 365 Data Handling Standards. Office 365 has conducted security categorization for its information and information systems, and the results are documented, reviewed, and approved by the authorizing official. Asset owners are responsible for maintaining up-to-date information regarding their assets. Customers are considered the owners of their data as it exists in Office 365.
Data Security & Information Lifecycle Management *Secure Disposal* DSI-07	*Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.*	Microsoft uses best practice procedures and a media wiping solution that is NIST 800-88 compliant when disposing of media. For hard drives that can't be wiped, Microsoft uses a destruction process that destroys the media (e.g., disintegrate, pulverize, or incinerate) and renders the recovery of information impossible. The appropriate means of disposal is determined by the asset type. Records of the destruction are retained.

Encryption and Key Management: Controls EKM-01 through EKM-04

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Encryption & Key Management *Entitlement* EKM-01	*Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.*	Microsoft has policies, procedures, and mechanisms established for effective key management to support encryption of data in storage and in transmission for the key components of the Office 365 service. Specifically, the Microsoft Public Key Infrastructure Operational Security Standard (PKI OSS) supports procedures including binding keys to specific owners.
Encryption & Key Management *Key Generation* EKM-02	*Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.*	The Microsoft PKI OSS defines the policies and procedures that define key management. The Standard accounts for various aspects of the key lifecycle, including the following procedures: • Classify the Impact Level of Certification Authority Procedure • Configure Security Monitoring for Servers and Devices Procedure • Define Standard Server Security Configuration for Certification and Registration Authorities Procedure • Define Trusted and Authorized Roles Procedure • Delete Certification Authority Cryptographic Keys Securely Procedure • Dispose of Hardware Security Modules and Related Tokens or Cards Securely Procedure • Dispose of Storage Devices and Media Securely Procedure • Document and Maintain Security Architecture Procedure • Document Certification Authority Hierarchy Procedure • Ensure Availability of Certificate Status Information Procedure • Ensure Certificates Comply with Minimum Certificate Profile Procedure • Establish Certification Practices Procedure • Evaluate Risks of Non-User Domain Accounts Procedure • Isolate Certification Authority System Network Procedure • Issue Certificates to External Parties Securely Procedure • Issue Server Authentication Certificates Securely Procedure • Keep Software Current and Install Security Updates Procedure • Log Key and Certificate Lifecycle Events Procedure • Maintain Audit Records and Inventories Securely Procedure • Maintain Hardware Security Modules Inventory Procedure • Maintain Server Inventory for Certification and Registration Authorities Procedure • Minimize Network Exposure of Certification Authorities Procedure • Model Threats to the Certification Authority/RA System Procedure • Physically Protect Certification Authority System Servers and Network Devices Procedure • Periodically Review Audit Records Procedure • Physically Protect Hardware Security Modules and Related Tokens or Cards Procedure • Physically Protect PKI Facilities Procedure • Plan and Follow Certification Authority Key Generation Ceremony Procedure • Plan Business Continuity and Disaster Recovery Procedure • Plan Security Incident Response Procedure • Protect Against Malicious Code Procedure • Restrict Subordinate CA Certificate Usage Procedure • Review Proposed Operational Changes Procedure • Securely Back up Certification Authority Cryptographic Keys Procedure • Segregate Sensitive Operational Roles Procedure
Encryption & Key Management *Sensitive Data Protection* EKM-03	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission*	Customer data in transit is protected using TLS. Office 365 is configured to negotiate FIPS compliant TLS protocols with supported client browsers, though non-FIPS compliant protocols are supported for legacy browser support. The Office 365 FIPS 140-2 encryption modules used for transmitted information are certified by NIST via certificates 1334, 1335, and 1336.

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
	(e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Office 365 uses BitLocker to encrypt customer data at rest at the volume-level. BitLocker encryption is a data protection feature that is integrated with Windows. BitLocker is one of the technologies used to safeguard against threats in case there are lapses in other processes or controls (e.g., access control or recycling of hardware) that could lead to someone gaining physical access to disks containing customer data. In this case, BitLocker eliminates the potential for data theft or exposure as a result of lost, stolen, or inappropriately decommissioned computers and disks. BitLocker is deployed with Advanced Encryption Standard (AES) 128-bit+ encryption on disks containing customer content in Exchange Online, SharePoint Online, and Skype for Business applications in Office 365 enterprise service. New servers are deployed using AES 256-bit and 128-bit encryption is being phased out. BitLocker key management involves the management of recovery keys that are used to unlock/recover encrypted disks in an Office 365 datacenter. Office 365 stores the master keys in a secured share, only accessible by individuals who have been screened and approved. The credentials for the keys are stored in a secret store, which requires a high level of elevation and approvals to access. All elevated access is both approved and logged by a group other than the group requesting access. For additional information, see the white paper Data Encryption Technologies, which is available for download from the STP. Office 365 uses Windows servers for its services. The Windows Server operating system has protections in place for preventing code execution in restricted memory locations, including: No Execute (NX), Address Space Layout Randomization (ASLR), and Data Execution Prevention (DEP). Additionally, the Microsoft SDL requires secure coding practices including explicit consideration for safe memory handling requirements.
Encryption & Key Management *Storage and Access* EKM-04	*Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.*	Office 365 uses a variety of encryption technologies for securing data, and provides scenarios for both Microsoft-managed keys and customer-imported keys (e.g., bring your own key aka control your own key). For specific information on the encryption technologies and the methods for managing the crypto keys, see the white paper Data Encryption Technologies, which is available for download from the STP.

Governance and Risk Management: Controls GRM-01 through GRM-11

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Governance and Risk Management *Baseline Requirements* GRM-01	*Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business need.*	Office 365 service teams develop, document, and maintain under configuration control a current baseline configuration of their production systems. Baseline images are reviewed at least annually and changes to baseline images are reviewed and approved before they are moved into production.
Governance and Risk Management *Data Focus Risk Assessments* GRM-02	*Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:* *• Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure* *• Compliance with defined retention periods and end-of-life disposal requirements* *• Data classification and protection from unauthorized use, access, loss, destruction, and falsification*	Office 365 conducts multiple risk assessments annually. Risk assessments are conducted by independent auditors as part of a formal audit, and by internal compliance and risk teams within Microsoft. Internal risk assessments are conducted in accordance with the NIST 800-30 standard. Vulnerabilities identified and cataloged during the risk assessments are based on NIST 800-30, NIST 800-53, and National Vulnerability database (U.S. government repository of standards-based vulnerability management data) guidance. The risk assessments include data collected in interviews, audits, and design specifications, and as part of the Office 365 continuous monitoring program. The level of risk is assessed by evaluating collected risk-related attributes regarding threats, vulnerabilities, assets and resources, current controls, and the associated likelihood that vulnerability could be exploited by a potential threat and the potential impact (for example, the potential magnitude of loss resulting from such exploitation).
Governance and Risk Management *Management Oversight* GRM-03	*Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.*	Office 365 staff participate in an annual security training program. They are recipients of periodic security awareness updates when applicable. Security education is an on-going process and is conducted regularly in order to minimize risks. While all Office 365 employees take mandatory security training, staff with potential to elevate access take specific security training appropriate for the services and role they perform.
Governance and Risk Management *Management Program* GRM-04	*An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business:* • *Risk management* • *Security policy* • *Organization of information security* • *Asset management* • *Human resources security* • *Physical and environmental security* • *Communications and operations management* • *Access control* • *Information systems acquisition, development, and maintenance*	An ISMP has been established to enable Office 365 to maintain and improve its management system for information security. Through establishment of the ISMP, Office 365 plans for and manages protection of its assets to acceptable security levels based on defined risk management processes. In addition, Office 365 monitors the ISMS and the effectiveness of controls in maintaining the confidentiality, integrity and availability of assets to continuously improve information security. The ISMS framework encompasses industry best-practices for information security and privacy. The ISMS has been documented and communicated in a customer-facing Information Security Policy, which can be made available upon request (customers and prospective customers must have a signed NDA or equivalent in place to receive a copy). Office 365 performs annual ISMS reviews, the results of which are reviewed by management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Governance and Risk Management *Management Support / Involvement* GRM-05	*Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.*	Office 365 has designed and implemented an ISMS framework that addresses industry best-practices for information security and privacy. The ISMS has been documented and communicated in a customer-facing Information Security Policy, which can be made available upon request (customers and prospective customers must have a signed NDA or equivalent in place to receive a copy). This policy is reviewed and approved annually by Office 365 management, who has established roles and responsibilities to oversee implementation of the policy. Each management-endorsed version of the Information Security Policy and subsequent updates are distributed to relevant stakeholders. The Information Security Policy is made available to new and existing Office 365 employees for review as part of an information security education and awareness program. Office 365 employees confirm that they have reviewed, and agree to adhere to, all policies within the Information Security Policy as part of their annual security training. Office 365 Contractor Staff also agree to adhere to the relevant policies within the Information Security Policy.
Governance and Risk Management *Policy* GRM-06	*Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.*	A customer facing version of the Information Security Policy is available for download from the STP. The Information Security Policy is made available to new and existing Office 365 employees for review as part of an information security education and awareness program. Office 365 employees confirm that they have reviewed, and agree to adhere to, all policies within the Information Security Policy as part of their annual security training. Office 365 Contractor Staff also agree to adhere to the relevant policies within the Information Security Policy.
Governance and Risk Management *Policy Enforcement* GRM-07	*A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.*	Office 365 services staff suspected of committing breaches of security and/or violating the Information Security Policy equivalent to a Microsoft Code of Conduct violation are subject to an investigation process and appropriate disciplinary action up to and including termination. Contracting staff suspected of committing breaches of security and/or violations of the Information Security Policy are subject to formal investigation and action appropriate to the associated contract, which may include termination of such contracts. Microsoft Human Resources is responsible for coordinating disciplinary responses.
Governance and Risk Management *Policy Impact on Risk Assessments* GRM-08	*Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.*	Office 365 performs risk assessments of its environment to review the effectiveness of information security controls and safeguards, as well as to identify new risks. The risks are assessed annually and the results of the risk assessment are presented to management through a formal risk assessment report.
Governance and Risk Management *Policy Reviews* GRM-09	*The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.*	The Information Security Policy undergoes a formal management review and update process at least annually. In the event that a significant change is required in the security policy, it may be reviewed and updated outside of the regular schedule.
Governance and Risk Management *Risk Assessments* GRM-010	*Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with*	Office 365 performs an annual formal risk assessment. As part of the overall ISMS framework, baseline security requirements are constantly being reviewed, improved and implemented. The Office 365 controls for risk and vulnerability assessment of the Office 365 infrastructure encompass all areas in this section and meet the requirements of the standards against which we audit, as demonstrated by reports identified on the Office 365 Trust Center.

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
	inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	
Governance and Risk Management *Risk Management Framework* GRM-11	*Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.*	Office 365 has established a risk management framework, and related processes, for assessing the applicable IT risks and 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. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.

Human Resources: Controls HRS-01 through HRS-11

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Human Resources *Asset Returns* HRS-01	*Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.*	Employees, contractors, and third-party users are formally notified to destroy or return, as applicable, any physical materials that Microsoft has provided to them during the term of employment or the period of contractor agreement and any electronic media must be removed from contractor or third-party infrastructure. Microsoft may also conduct an audit to make sure data is removed in an appropriate manner.
Human Resources *Background Screening* HRS-02	*Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.*	Pursuant to local laws, regulations, ethics, and contractual constraints, Microsoft US-based FTEs are required to successfully complete a standard background check as part of the hiring process. Background checks may include but are not limited to review of information relating to a candidate's education, employment, and criminal history. Third-party contractors are subject to the hiring practices of their organizations, and contractor agencies must adhere to equivalent standards exercised by Microsoft.
Human Resources *Employment Agreements* HRS-03	*Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.*	Microsoft has developed and documented confidentiality and non-disclosure agreements, as well as the Microsoft Employee Handbook access agreements, which all Office 365 staff are required to sign as a condition for employment and access to the Office 365 system. Microsoft has also developed the Master Supplier Services Agreement (MSSA) that vendors and contractors are required to sign to ensure compliance with Microsoft policies on required engagements.
Human Resources *Employment Termination* HRS-04	*Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.*	Microsoft Corporate Human Resources Policy drives employee termination processes and clearly defines roles and responsibilities. Termination policies and procedures cover all aspects of separation including return of assets, badges, computer equipment and data. Human Resources also manages revocation of access to resources, both physical and electronic.
Human Resources *Mobile Device Management* HRS-05	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).*	Office 365 teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to be connected to the production environment. Mobile computing access points on the Microsoft corporate network are required to adhere to wireless device security requirements.
Human Resources *Non-Disclosure Agreements* HRS-06	*Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.*	Microsoft Legal and Human Resources maintain policies and procedures defining the implementation and execution of non-disclosure and confidentiality agreements.
Human Resources *Roles / Responsibilities* HRS-07	*Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.*	The Information Security Policy exists in order to provide Microsoft staff and contractor staff with a current set of clear and concise Information Security Policies including their roles and responsibilities related to information assets and security. These policies provide direction for the appropriate protection of Office 365. The Information Security Policy has been created as a component of an overall ISMS for Office 365.
Human Resources *Technology Acceptable Use* HRS-08	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile*	Mobile and wireless devices are not permitted within Microsoft datacenters where customer data is stored. Wireless access to Office 365 production environments is prohibited.

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
	devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	
Human Resources *Training / Awareness* HRS-09	*A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.*	All Office 365 staff take part in annual Office 365 sponsored security training program, and are recipients of periodic security awareness updates when applicable. Security education is an ongoing process and is conducted regularly in order to minimize risks. Additionally, Microsoft also has non-disclosure provisions in employee contracts.
Human Resources *User Responsibility* HRS-10	*All personnel shall be made aware of their roles and responsibilities for:* • *Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.* • *Maintaining a safe and secure working environment*	Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire and annually thereafter. In addition, employees must acknowledge the Microsoft Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, on an annual basis.
Human Resources *Workspace* HRS-11	*Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.*	Microsoft Security Policy requires that all users lock their workstations when leaving them unattended. Office 365 personnel accounts have session lock policies that enforce session lockouts after a defined period of inactivity. Remote Desktop boundary protection devices also limit the amount of time a network session can be maintained with a production server. Network connections are terminated after that defined period of inactivity.

Identity and Access Management: Controls IAM-01 through IAM-13

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Identity & Access Management *Audit Tools Access* IAM-01	*Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.*	Log and monitor access is highly restricted to only authorized staff with a business need to access such systems. Access to such data requires approval before permissions are granted. Systems that monitor and alert on audit data are segmented at the network and host layer and access is restricted to limited authorized staff via Role Based Access Control (RBAC).
Identity & Access Management *Credential Lifecycle / Provision Management* IAM-02	*User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following:* • *Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships)* • *Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems)* • *Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant))* • *Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation)* • *Account credential lifecycle management from instantiation through revocation* • *Account credential and/or identity store minimization or re-use when feasible* • *Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets)* • *Permissions and supporting capabilities for customer (tenant) controls over*	Log and monitor access is highly restricted to only authorized staff with a business need to access such systems. Access to such data requires approval before permissions are granted. Systems that monitor and alert on audit data are segmented at the network and host layer and access is restricted to limited authorized staff via RBAC. Office 365 has adopted applicable corporate and organizational security policies, including the Information Security Policy. The policies have been approved, published and communicated across Office 365 teams. The Information Security Policy requires that access to Office 365 assets to be granted based on business justification, with the asset owner's authorization and limits based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. Access to Microsoft buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into Datacenters. Front desk personnel are required to positively identify FTEs or authorized contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. Guests must be escorted by authorized Microsoft personnel. Password policies for corporate domain accounts are managed through Microsoft corporate Active Directory policy that specifies minimum requirements for password length, complexity, and expiry. Accounts for Office 365 personnel are managed through Microsoft's corporate Active Directory. Security group membership must be approved by the designated security group owners within Office 365. Office 365 has implemented multifactor authentication for all network access by Office 365 personnel through the use of smart cards and TPM modules. All Microsoft users connect to the system via Terminal Server Gateways (TSGs) and the TSGs require the user to present a certificate bound to the card (something you have) with a PIN (something you know). In the case of a terminating user, automated procedures are in place to disable the user's Active Directory accounts upon termination. Accounts with access to Office 365 are also disabled after 90 days of inactivity.

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
	authentication, authorization, and accounting (AAA) rules for access to • *data and sessions* • *Adherence to applicable legal, statutory, or regulatory compliance requirements*	
Identity & Access Management *Diagnostic / Configuration Ports Access* IAM-03	*User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.*	Access control policy is a component of overall policies and undergoes a formal review and update process. Access to Office 365 assets is granted based upon business requirements and with the asset owner's authorization. Additionally: • Access to assets is granted based upon need-to-know and least-privilege principles. • Role-based access controls are used to allocate logical access to a specific job function or area of responsibility, rather than to an individual. • Physical and logical access control policies are consistent with standards. The Microsoft MCIO team controls physical access to diagnostic and configuration ports through physical datacenter controls. Diagnostic and configuration ports are only accessible by arrangement between service and asset owners, and hardware and software support personnel requiring access. Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, are disabled or removed.
Identity & Access Management *Policies and Procedures* IAM-04	*Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.*	In support of the Access Control requirements in the Information Security Policy, Office 365 maintains Active Directory deployments for identifying and authenticating Microsoft users in the environment. Office 365 personnel accessing the Office 365 system are uniquely identified by their Active Directory username and authenticate using two-factor authentication. Active Directory strictly enforces unique identifiers and logs activities attempted and executed by each user.
Identity & Access *Management* *Segregation of Duties* IAM-05	*User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.*	In support of the Information Security Policy, Office 365 service teams defined roles as part of a comprehensive RBAC access model. Each service team has identified roles that, if shared by a single person, would allow for malicious activity without collusion. When such role pairs exist, no individual is allowed to belong to both roles. Account permissions and role access are reviewed as part of an annual account review process.
Identity & Access Management *Source Code Access Restriction* IAM-06	*Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.*	Access to Office 365 source code libraries is limited to authorized personnel. Source code libraries enforce control over changes to source code by requiring a review from designated Office 365 staff prior to code check-in. An audit log detailing modifications to the source code library is maintained.
Identity & Access Management *Third Party Access* IAM-07	*The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.*	Identification, assessment, and prioritization of risks related to external parties and access controls is performed as part of the Office 365 risk management program and verified as part of the ISO 27001 audit. Third party security and privacy requirements are established through vendor due-diligence reviews, conducted by the designated Office 365 manager, and included in signed contractual agreements prior to engaging in third party services. The engaging team within Office 365 is responsible for managing their third party relationships, including contract management, monitoring of metrics such as service level agreements, and vendor access to relevant applications.
Identity & Access Management *Trusted Sources* IAM-08	*Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.*	Office 365 uses Active Directory to manage staff user accounts. Security group membership must be approved by the designated security group owners within Office 365. Automated procedures are in place to disable staff Active Directory accounts when staff users are terminated. Staff user accounts are disabled after 90 days of inactivity. Office 365 service teams employ the concept of least privilege, allowing only authorized accesses for service team users that are necessary to

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
		accomplish assigned tasks in accordance with business functions and organizational need.
Identity & Access Management *User Access Authorization* IAM-09	*Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	Office 365 uses Active Directory to manage and provision user accounts. Security group membership must be approved by the designated security group owners within Office 365. Automated procedures are in place to disable Active Directory accounts upon the user's leave date. Domain-level user accounts are disabled after 90 days of inactivity. Strong authentication, including the use of multi-factor authentication, helps limit access to customer data to authorized personnel only. Sample audits are performed by both Microsoft and third parties to attest that access is only for appropriate business purposes. When access is granted, it is carefully controlled and logged, and revoked as soon as it is no longer needed. The operational processes and controls that govern access and use of customer data in Office 365 are rigorously maintained and regularly verified by independent auditors.
Identity & Access Management *User Access Reviews* IAM-10	*User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.*	The Information Security Policy requires that access to Office 365 assets be granted based on business justification, with the asset owner's authorization and limited based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. Managers and owners of applications and data are responsible for reviewing who has access on a periodic basis. Customers control access of their users and are responsible for ensuring appropriate review of such access.
Identity & Access Management *User Access Revocation* IAM-11	*Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	Designated security group owners within Office 365 are responsible for reviewing appropriateness of employee access to applications and data on a regular basis. Regular access review audits occur to validate appropriate access provisioning has taken place. Access is modified based on the results of this review. Membership in security groups must be approved by security group owners. In case of a user who changes roles and no longer works within Office 365, their account is removed from any security groups that have access to Office 365 services. In the case of user termination, automated procedures are in place to disable a user's Active Directory account when a user is terminated.
Identity & Access Management *User ID Credentials* IAM-12	*Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:* • *Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)* • *Account credential lifecycle management from instantiation through revocation* • *Account credential and/or identity store minimization or re-use when feasible* • *Adherence to industry acceptable and/or regulatory compliant authentication,*	Microsoft does not manage any customer (tenant) accounts or access control. Office 365 provides customers with the necessary tools and features to control their own accounts and perform their own identity management. Customers are responsible for keeping customer passwords from being disclosed to unauthorized parties and for choosing passwords with sufficient entropy as to be effectively non-guessable and for deployment of services such as multi-factor authentication. As for Microsoft corporate accounts that have access to Office 365, Microsoft maintains Active Directory deployments for identifying and authenticating Microsoft users in the environment. Office 365 personnel accessing the Office 365 system are uniquely identified by their Active Directory username and authenticate using two-factor authentication. Active Directory strictly enforces unique identifiers and logs activities attempted and executed by each user.

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
	authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	In the case of a terminated user, automated procedures are in place to disable the user's Active Directory accounts upon termination. Microsoft staff accounts with access to Office 365 are disabled after 90 days of inactivity. Office 365 has configured Active Directory to ensure that authenticators must comply with Windows strong password requirements and meet certain password length requirements. In addition, Windows strong passwords must contain characters from at least three of these four: • English lowercase • English uppercase • Numbers (0-9) • Special characters Active Directory also enforces a maximum password age which is configured to no more than 60 days per domain. Additionally, Active Directory enforces a minimum password age of one day.
Identity & Access Management *Utility Programs Access* IAM-13	*Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.*	Utility programs undergo changes through the release management process and are restricted to authorized personnel only. Guardrails are put in place to assure specific utility programs have the least privileges necessary to perform the business function they are approved to perform. Monitoring and alerting is in place for all utility programs. In the event that an alert is generated a security incident investigation ticket is opened and assigned to the Office 365 Incident Response team for investigation.

Interoperability and Portability: Controls IPY-01 through IPY-05

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Interoperability & Portability *APIs* IPY-01	*The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.*	Office 365 supports a set of API's to allow customers to access Office 365 data including their mail, calendars, contacts, files, and folders. For more information regarding Office 365 API's please see the Office 365 APIs Platform Overview.
Interoperability & Portability *Data Request* IPY-02	*All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files)*	Customers can access their data at any time and for any reason without assistance from Microsoft. Microsoft will use customer data only to provide the services agreed upon, including purposes that are compatible with providing those services. Office 365 provides authenticated and logged access to customer data which restricts access to it by Microsoft personnel and subcontractors. We also take strong steps to protect your customer data from inappropriate use or loss, and to segregate customer data on shared hardware from that of other customers.
Interoperability & Portability *Policy & Legal* IPY-03	*Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.*	Office 365 supports a set of API's to allow customers to access Office 365 data including their mail, calendars, contacts, files, and folders. For more information regarding Office 365 API's please see the Office 365 APIs Platform Overview.
Interoperability & Portability *Standardized Network Protocols* IPY-04	*The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.*	Customers are responsible for ensuring a secure connection to the Office 365 system for the purpose of importing and exporting data. For an overview of the Office 365 APIs platform please see the Office 365 APIs Platform Overview.
Interoperability & Portability *Virtualization* IPY-05	*The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.*	Office 365 uses both physical servers and virtualized servers. Virtualized servers use industry-standard Microsoft virtualization technologies. This includes the use of Microsoft Azure which employs virtual servers leveraged by Office 365. For more information, see Microsoft Azure Virtual Machines.

Infrastructure and Virtualization Security: Controls IVS-01 through IVS-13

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection* IVS-01	*Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.*	Office 365 uses monitoring agents to verify that audit logs are being generated and being uploaded to a centralized log monitoring service. Audit processing failures generate alerts that are reported to Service Engineer Operations personnel and escalated to Office 365 Security as appropriate. Audit logs are retained in accordance with the Office 365 Data Handling Standard, and access is restricted to staff that have a business need to access the logs. Audit log access is reviewed on a regular basis to ensure access is necessary.
Infrastructure & Virtualization Security *Change Detection* IVS-02	*The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g. portals or alerts).*	Each OS is deployed via a “Base Image” that is constructed through a formal build process. Each base image is built upon an OS version in which the kernel, and many other core components, have been modified and optimized to support the Office 365 environment. Virtual machines that are used within Office 365 have logging, monitoring, and alerting enabled such that unauthorized changes generate alerts which are followed up on by the service teams and Office 365 Security as necessary. All changes to the baseline images are approved through a formal approval process and the baselines are routinely reviewed to assure integrity of the builds.
Infrastructure & Virtualization Security *Clock Synchronization* IVS-03	*A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.*	All Office 365 servers regularly synchronize time from MCIO or NIST time servers. The MCIO time servers are NTP Stratum 1 time servers that synchronize off of the Global Positioning System satellites. MCIO and NIST both manage multiple NTP time servers in separated geographic locations.
Infrastructure & Virtualization Security *Information System Documentation* IVS-04	*The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.*	Office 365 service teams include capacity planning as a key feature of their datacenter models and data replication plans to ensure that there is sufficient capacity for information processing, telecommunications, and environmental support. Capacity is reviewed at least monthly.
Infrastructure & Virtualization Security *Management - Vulnerability Management* IVS-05	*Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware).*	Procedures have been established and implemented to regularly scan for vulnerabilities on all virtual and non-virtual assets. Vulnerability scanning is performed on server operating systems, databases, and network devices with the appropriate vulnerability scanning tools. The vulnerability scans are performed on a quarterly basis at a minimum. Office 365 contracts with independent assessors to perform penetration testing of the Office 365 boundary. Internal Office 365 Red Team versus Blue Team exercises are also routinely performed and results used to make security improvements.
Infrastructure & Virtualization Security *Network Security* IVS-06	*Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls.*	Firewall rules and access control lists (ACL) are documented and reviewed on at least a quarterly basis. Changes are required to follow the approved firewall rule change control process. Traffic flow policies are implemented on boundary protection devices that deny traffic by default. These policies are reviewed every month to determine if any changes are required.
Infrastructure & Virtualization Security *OS Hardening and Base Controls* IVS-07	*Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.*	The Office 365 team leverages United States Government Configuration Baseline (USGCB) and Center for Internet Security (CIS) Benchmarks in the development of their base images. Operating system images are hardened restricting services, ports and protocols to the minimum set necessary for business functionality. The use of anti-malware software is a principal mechanism for protection of Office 365 assets from malicious software. The anti-malware software detects and prevents the introduction of computer viruses, malware, rootkits, worms, and other

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
		malicious software onto the service systems. Anti-malware software provides both preventive and detective control over malicious software. Anti-malware software is installed as part of the initial build on all systems.
Infrastructure & Virtualization Security *Production / Non-Production Environments* IVS-08	*Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.*	For the Office 365 infrastructure, production and non-production environments are both physically and logically separated. Office 365 employs network-based and host-based boundary protection devices such as firewalls, load balancers, IP Filters, and front-end components to achieve this logical separation. Additionally, access to both environments is controlled using Role Based Access Controls so that only authorized personnel may logically access the intended environment. All access to the production environment requires multi-factor authentication.
Infrastructure & Virtualization Security *Segmentation* IVS-09	*Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations:* • *Established policies and procedures* • *Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance* • *Compliance with legal, statutory and regulatory compliance obligations*	Multiple forms of protection have been implemented throughout Office 365 to prevent customers from compromising Office 365 services or applications or gaining unauthorized access to the information of other tenants or the Office 365 system itself: • Logical isolation of tenant data for all Office 365 workloads is achieved through Azure Active Directory authorization and role-based access control. • SharePoint Online provides data isolation mechanisms at the storage level. • Office 365 also uses rigorous physical security, background screening, and a multi-layered encryption strategy to protect the confidentiality and integrity of customer data. ○ All Office 365 and datacenters have biometric access controls, with the majority of the datacenters used to provide Office 365 requiring palm prints to gain physical access, and all U.S.-based Microsoft employees are required to successfully complete a standard background check as part of the hiring process. For more information on data access security measures, see Administrative Access. ○ Office 365 uses service-side technologies that encrypt customer data at rest and in transit. For customer data at rest, Office 365 uses volume-level and file-level encryption. For customer data in-transit, Office 365 uses multiple encryption technologies for communications between datacenters and between clients and servers, such as Transport Layer Security (TLS), and Internet Protocol Security (IPsec). For specific details on the encryption mechanisms used throughout Office 365, see Data Encryption Technologies in Office 365, available from the STP. Together, these protections provide robust logical isolation controls that provides equivalent threat protection and mitigation to that provided by physical isolation alone. Office 365 also employs a defense-in-depth strategy for boundary protection, including secure segmentation of network environments through several methods including VLANs, ACL restrictions, and encrypted communications for remote connectivity.
Infrastructure & Virtualization Security *VM Security - vMotion Data Protection* IVS-10	*Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.*	Office 365 uses encryption to protect the integrity and confidentiality of transmitted information. Connections to interconnected systems are made using strictly enforced FIPS 140-2, Level 2-validated TLS protocols.
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening* IVS-11	*Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated*	Where virtualization is used, Office 365 enforces the concept of least privilege and restricts access to information systems including the hypervisor or hypervisor management plane using role based security groups.

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
	communications to the administrative consoles).	
Infrastructure & Virtualization Security *Wireless Security* IVS-12	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following:* • *Perimeter firewalls implemented and configured to restrict unauthorized traffic* • *Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings)* • *User access to wireless network devices restricted to authorized personnel* • *The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network*	Office 365 does not permit or allow wireless connections in the Office 365 network environment.
Infrastructure & Virtualization Security *Network Architecture* IVS-13	*Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.*	Internal Office 365 data flow diagrams clearly define boundaries and data flows between zones having different data classification, trust levels, or compliance and regulatory requirements. Communication channels are logically or physically isolated from other networks. Customer information is encrypted during transmission over external networks. Network filtering is implemented to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted platform components. Office 365 sits behind load balancers and traffic filters to control the flow of traffic. Additionally, Office 365 has established automated controls to monitor and detect internally initiated denial of service attacks. For more information about how Microsoft protects Office 365 from denial of service attacks, see Defending Office 365 Against Distributed Denial of Service Attacks, available for download from the STP.

Mobile Security: Controls MOS-01 through MOS-20

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Mobile Security *Anti-Malware* MOS-01	*Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.*	Mobile and wireless devices are not permitted within Microsoft datacenters where customer data is stored. Wireless access to Office 365 production and customer environments is prohibited.
Mobile Security *Application Stores* MOS-02	*A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.*	See response to MOS-01.
Mobile Security *Approved Applications* MOS-03	*The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.*	See response to MOS-01.
Mobile Security *Approved Software for BYOD* MOS-04	*The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.*	See response to MOS-01.
Mobile Security *Awareness and Training* MOS-05	*The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.*	See response to MOS-01.
Mobile Security *Cloud Based Services* MOS-06	*All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.*	See response to MOS-01.
Mobile Security *Compatibility* MOS-07	*The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.*	See response to MOS-01.
Mobile Security *Device Eligibility* MOS-08	*The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.*	See response to MOS-01.
Mobile Security *Device Inventory* MOS-09	*An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)) will be included for each device in the inventory.*	See response to MOS-01.
Mobile Security *Device Management* MOS-10	*A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.*	See response to MOS-01.
Mobile Security *Encryption* MOS-11	*The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.*	See response to MOS-01.

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Mobile Security *Jailbreaking and Rooting* MOS-12	*The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and shall enforce the prohibition through detective and preventative controls on the device or through a centralized device management system (e.g. mobile device management).*	See response to MOS-01.
Mobile Security *Legal* MOS-13	*The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations regarding the loss of non-company data in the case a wipe of the device is required.*	See response to MOS-01.
Mobile Security *Lockout Screen* MOS-14	*BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.*	See response to MOS-01.
Mobile Security *Operating Systems* MOS-15	*Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.*	See response to MOS-01.
Mobile Security *Passwords* MOS-16	*Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.*	See response to MOS-01.
Mobile Security *Policy* MOS-17	*The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).*	See response to MOS-01.
Mobile Security *Remote Wipe* MOS-18	*All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.*	See response to MOS-01.
Mobile Security *Security Patches* MOS-19	*Mobile devices connecting to corporate networks, or storing and accessing company information, shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.*	See response to MOS-01.
Mobile Security *Users* MOS-20	*The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.*	See response to MOS-01.

Security Incident Management, E-discovery, and Cloud Forensics: Controls SEF-01 through SEF-05

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance* SEF-01	*Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.*	Office 365 has designated responsibilities and established processes to maintain contacts with external authorities across the jurisdictions in which it operates.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management* SEF-02	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.*	Policies and procedures are authorized by management which support a tiered triage model of security related events. Potential security issues are investigated and escalated as appropriate in accordance with the internal Office 365 Security Incident Response plan.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting* SEF-03	*Workforce personnel and external business relationships shall be informed of their responsibilities and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.*	Microsoft Rules of Behavior describes Microsoft users' responsibilities and establishes expected behavior when using Office 365 and other Microsoft systems. All Microsoft users, including employees, vendors, and contractors are required to follow the rules of behavior, which are outlined in the Rules of Behavior agreement. The agreements set expectations about proper use of the system and include requirements that staff report security events in a timely manner.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Legal Preparation* SEF-04	*Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.*	In the event a follow-up action concerning a person or organization after an information security incident requires legal action, proper forensic procedures including chain of custody shall be required for preservation and presentation of evidence to support potential legal action subject to the relevant jurisdiction. Upon notification of a security breach, impacted customers (tenants) and other external business relationships shall be given the opportunity to participate as is legally permissible in the forensic investigation. Security incident response plans and collection of evidence adheres to ISO 27001 standards. Office 365 has established processes for evidence collection and preservation for troubleshooting an incident and analyzing the root cause. In case a security incident involves legal action such as subpoena form, the guidelines described in the trouble shooting guide are followed.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Metrics* SEF-05	*Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.*	An incident management framework has been established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents. Incident management teams perform constant monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. Events, thresholds and metrics have been defined and configured to detect incidents and alert the appropriate Office 365 teams and management.

Supply Chain Management, Transparency and Accountability: Controls STA-01 through STA-09

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity* STA-01	*Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.*	Microsoft requires all third parties (external information system services) who are engaged with Office 365 to sign a MSSA. The MSSA requires the third party to comply with all applicable Microsoft security policies and implement security procedures to prevent disclosure of confidential Microsoft information. Microsoft includes provisions in the MSSA and any associated Statements of Work (SOW) with each vendor addressing the need to employ appropriate security controls. Vendors that handle sensitive data must be in compliance with Microsoft vendor privacy practices and data protection requirements.
Supply Chain Management, Transparency and Accountability *Incident Reporting* STA-02	*The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).*	The Office 365 process for managing a security incident conforms to the approach prescribed by NIST 800-61. Microsoft's security incident response includes several dedicated teams that work together to prevent, monitor, detect, and respond to security incidents. Office 365 maintains and notifies customers of potential changes and events that may affect security or availability of the services through an online Service Dashboard. Service health information is available at any time by signing into Office 365. Changes to the security commitments and security obligations of Office 365 customers are updated on the Office 365 website in a timely manner. For more information, see Office 365 Security Incident Management, available for download from the STP.
Supply Chain Management, Transparency and Accountability *Network / Infrastructure Services* STA-03	*Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.*	Office 365 employs sophisticated software-defined service instrumentation and monitoring that integrates at the component or server level, the datacenter edge, our network backbone, Internet exchange sites, and at the real or simulated user level, providing visibility when a service disruption is occurring and pinpointing its cause. Proactive monitoring continuously measures the performance of key subsystems of the Office 365 services platform against the established boundaries for acceptable service performance and availability. When a threshold is reached or an irregular event occurs, the monitoring system generates warnings so that operations staff can address the threshold or event.
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments* STA-04	*The provider shall perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.*	Office 365 performs risk assessments of its environment to review the effectiveness of information security controls and safeguards, as well as to identify new risks. The risks are assessed annually and the results of the risk assessment are presented to management through a formal risk assessment report. Supplier scorecards have been developed to allow comparison and visibly monitor the performance of our suppliers using a balanced scorecard approach.
Supply Chain Management, Transparency and Accountability *Supply Chain Agreements* STA-05	*Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms:* • *Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any*	Third party security and privacy requirements are established through vendor due-diligence reviews, conducted by the designated Office 365 manager, and included in signed contractual agreements prior to engaging in third party services. The engaging team within Office 365 is responsible for managing their third party relationships, including contract management, monitoring of metrics such as service level agreements, and vendor access to relevant applications.

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
	known regulatory compliance considerations) • *Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships* • *Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts* • *Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain)* • *Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit* • *report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed* • *Expiration of the business relationship and treatment of customer (tenant) data impacted* • *Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence*	
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews* STA-06	*Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.*	Security risks related to external parties, such as customers, contractors and vendors are identified and addressed through the following: 1. Customer risks are assessed in coordination with Microsoft's in-house legal department (known as Corporate, External, and Legal Affairs (CELA)) and appropriate customer agreements are established. 2. Third parties undergo a review process through Global Procurement and an approved vendor list has been established. Purchase orders to engage a third-party require a MSSA to be established or a review to be performed by CELA. Vendors requiring access to source code need to be approved by the GM and CELA, and sign a Source Code Licensing Agreement. 3. Additional risks related to granting access to facilities and information systems are controlled and managed by Microsoft internal IT. Physical and network security for offsite vendor facilities are governed by Microsoft.
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics* STA-07	*Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify any non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or*	Office 365 has established procedures and designated responsibilities for managing changes to third-party services. Office 365 has designated teams that manage third-party relationships including contract management, monitoring metrics such as service-level agreements, and third party access to systems, in accordance with these procedures as well as corporate-wide third party management processes. The services provided by third-party vendors are monitored against the service levels by designated responsible persons in Office 365, as defined in the SOW. Procedures for monitoring breaches to contractual obligations and handling issues with vendors are established.

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
	inconsistencies resulting from disparate supplier relationships.	
Supply Chain Management, Transparency and Accountability *Third Party Assessment* STA-08	*Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party-providers upon which their information supply chain depends on.*	Office 365 contractually requires that its subcontractors meet important privacy and security requirements. Requirements and contracts are reviewed at least annually or as renewed.
Supply Chain Management, Transparency and Accountability *Third Party Audits* STA-09	*Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.*	The services provided by third-party vendors are monitored against the service levels by designated responsible persons from Office 365 and contractually requires that its subcontractors meet important privacy and security requirements. Third party service providers are routinely audited by both Microsoft and independent audit teams.

Threat and Vulnerability Management: Controls TVM-01 through TVM-03

(Go to Table of Contents)

CCM Control Domain and ID	CCM v3.0.1 Control Specification	Office 365 Response
Threat and Vulnerability Management *Anti-Virus / Malicious Software* TVM-01	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	In support of the Information Security Policy, Office 365 runs multiple layers of anti-virus software to ensure protection from common malicious software. Servers within the Office 365 environment run anti-virus software that scans files uploaded and downloaded from the service for viruses or other malware. Additionally, all mails coming into the service run through the Exchange Online Protection engine, which uses multiple antivirus and antispam engines to capture known and new threats against the system. Additional information may be found in the relevant service descriptions and Service Level Agreement (SLA). Microsoft has its own Security Response Center (MSRC) that also supplies information to all our customers covering the whole range Microsoft products. More information can be found at the Security TechCenter MSRC page.
Threat and Vulnerability Management *Vulnerability / Patch Management* TVM-02	*Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	Office 365 implements technologies to routinely scan the environment for vulnerabilities. Additionally, Office 365 contracts with external penetration testers who routinely scan the Office 365 system. Identified vulnerabilities are tracked, and verified for remediation. In addition, regular vulnerability and penetration assessments are performed to identify vulnerabilities and determine whether key logical controls are operating effectively. The MSRC regularly monitors external security vulnerability awareness sites. As part of the routine vulnerability management process, Office 365 evaluates our exposure to these vulnerabilities and leads action across Office 365 to mitigate risks when necessary. Per best practice, Microsoft has full, robust patch management systems that are audited and tracked regularly by management. Any issues or requested exceptions would require management approval to address. This process is included in the ongoing audit schedule.
Threat and Vulnerability Management *Mobile Code* TVM-03	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	The use of mobile code in Office 365 applications is reviewed during multiple phases of the SDL process. The SDL policy documents the usage restrictions and implementation guidance on mobile technologies such as ActiveX, Flash, Silverlight, and JavaScript. It also lists the outdated technologies that are not permitted in Office 365.