



Standard Response to Request for Information
> Security and Privacy

Disclaimer

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. For the latest version of this document visit: <http://www.microsoft.com/download/en/details.aspx?id=26647>

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2011 Microsoft Corporation. All rights reserved.

Microsoft and Microsoft Office 365 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

	Page
Introduction	4
How Office 365 is Delivered: The Services Stack	5
ISO Certifications for the Microsoft's Online Services Stack	6-8
Microsoft Response by Cloud Control Matrix ID:	9 -51
Compliance	CO-01 through CO-06
Data Governance	DG-01 through DG-08
Facility	FS-01 through FS-08
Human Resources	HR-01 through HR-03
Information Security	IS-01 through IS-34
Legal	LG-01 through LG-02
Operations	OP-02 through OP-03
Risk Management	RI-01 through RI-05
Release Management	RM-01 through RM-05
Resiliency	RS-01 through RS-08
Security Architecture	SA-01 through SA-15

The Cloud Security Alliance (CSA) is a not-for-profit organization promoting the use of best practices for security assurance within Cloud Computing.

The Cloud Security Alliance published the Cloud Control Matrix, to support consumers in the evaluation of cloud services and to identify questions prudent to have answered before moving to cloud services. In response to this publication, Microsoft Online Services has created this document to outline how we meet the suggested principles and mapped them to the ISO certification.

Learn more:

<https://cloudsecurityalliance.org>

Introduction

Computing in the cloud raises questions about security, data protection, privacy and data ownership. Microsoft® Office 365 (including Microsoft® Exchange Online, Microsoft® SharePoint Online, and Microsoft® Lync™ Online branded services) is hosted in Microsoft data centers, around the world and is designed to offer the performance, scalability, security and service levels business customers expect. We have applied state-of-the-art technology, and processes to maintain consistent and reliable access, security and privacy for every user. Microsoft Online Services has built-in capabilities for compliance with a wide range of regulations and privacy mandates.

In this document we provide our customers with a detailed overview of how Microsoft Online Services fulfill the security, privacy, compliance, and risk management requirements as defined in the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM). Note that this document is intended to provide information on how Microsoft Online Services operate. Customers have a responsibility to control and maintain their environment once the service has been provisioned (i.e. user access management and appropriate policies and procedures in accordance with their regulatory requirements).

Security requirements for the cloud: the Cloud Control Matrix.

The Cloud Control Matrix (CCM) is published by 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 matrix provides a detailed understanding of security and privacy, concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains.

Microsoft has published a detailed overview of our capabilities for the CCM requirements in this document. With this standard Request for Information (RFI) response we would like to illustrate and empower customers with in-depth information to evaluate different offerings in the market place today.

Introducing Office 365.

While Microsoft offers a range of cloud services, our objective here is to specifically provide answers for Microsoft's Office 365 hosted business service offering. Office 365 provides a set of productivity applications that bring together online versions of our email and collaboration software with our familiar Microsoft Office Professional Plus suite in the cloud. Office 365 applications run on a cloud infrastructure and are accessible from various client devices. Customers do not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage or the individual application capabilities with the exception of certain configuration capabilities. For more information, please visit www.office365.com.

How Office 365 is Delivered: The Services Stack

The Trust Center offers additional information on topics such as geo-location of data, administrator access, and expanded information about compliance practices.

To learn more visit our [Trust Center](#)

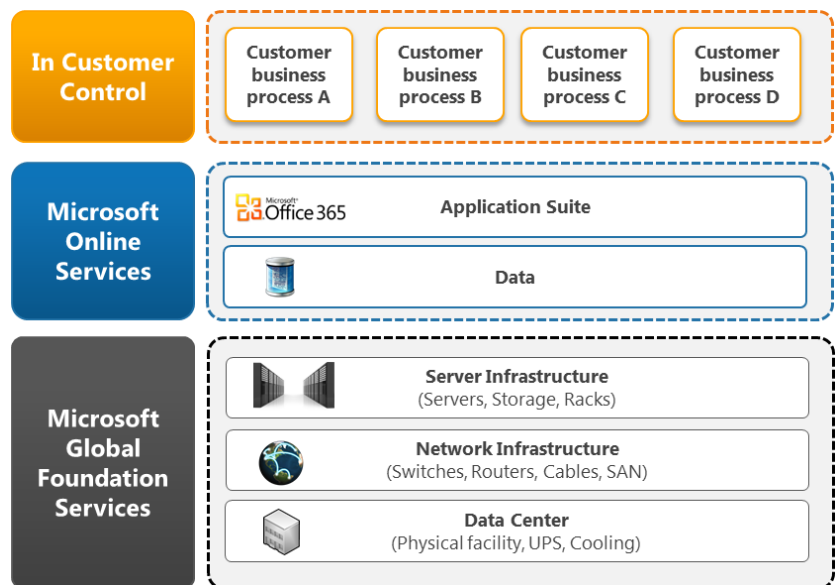
(<http://go.microsoft.com/fwlink/?LinkID=206613&CLCID=0x409>)

When evaluating the control environment in a Software-as-a-Service offering, it is important to consider the whole services stack of the cloud service provider. Many different organizations may be involved in providing infrastructure and application services, increasing the risk of misalignment. A disruption of any one layer in the stack could compromise the delivery of the cloud service and have disastrous impacts. As a result, customers should evaluate how their service provider operates, and understand the underlying infrastructure and platforms of the service as well as the actual applications.

Microsoft is a cloud service provider that owns and controls the entire stack, from the applications developed for the cloud, to the data centers that host your data and service, all the way to the fiber optic cable pathways that transport your information, and to the actual provisioning of the service.

In the Office 365 environment, the service is managed by the *Microsoft Global Foundation Services* group, who provides infrastructure services to both Microsoft customers as well as internally and the *Microsoft Online Services* group, which provides the application suite and data layer (see Figure 1).

Figure 1: The Services Stack for Office 365



ISO Certifications for the Microsoft Online Services Stack

Microsoft's ISO 27001 certifications enable customers to evaluate how Microsoft meets or exceeds the standards and implementation guidance.

Both Office 365 and the infrastructure on which it relies (Microsoft Global Foundation Services) employ security frameworks based on the International Standards Organization (ISO/IEC 27001:2005) family of standards and are ISO 27001 certified by independent auditors.

Our ISO 27001 certifications enable customers to evaluate how Microsoft meets or exceeds the standards and implementation guidance against which we are certified. ISO 27001 defines how to implement, monitor, maintain, and continually improve the Information Security Management System (ISMS). In addition, both the services and the infrastructure undergo a yearly SAS 70 (or successor SSAE16) audit.

The Microsoft Online Services Information Security Policy, applicable to Office 365, also aligns with ISO 27002, augmented with requirements specific to online services. ISO 27002 is not a certification but provides a suggested set of suitable controls for the Information Security Management System.

How to read CSA requirements and Microsoft's response

On the following pages, we have mapped our security practices to the guidance provided by the CCM. The first two columns, headed "Control ID in CCM" and "Description", consist of content directly from the CCM identifying relevant controls¹. The third column, headed "Microsoft Response" consists of:

- 1) A short explanation of how Microsoft Online Services satisfy the Cloud Security Alliance recommendation.
- 2) A reference to the ISO 27001 controls attested to by the Microsoft Global Foundation Services (GFS) and/or Microsoft Online Services ISO 27001 certifications, where relevant.

Example:

The Cloud Security Alliance Cloud Control Matrix, ID IS-O2 states:

"Executive and line management shall take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution."

Microsoft's Response:

"Each management-endorsed version of the Information Security Policy and all subsequent updates are distributed to all relevant stakeholders. The Information Security Policy is made available to all new and existing Microsoft Online Services employees for review."

(1) CCM content in columns 1 and 2 is © 2011 Cloud Security Alliance, used with permission.

The fact that Microsoft Online Services is certified to ISO 27001 means that we have been able to meet the external auditors' expectations that our environment meets or exceeds such standards.

The public copy of the Microsoft Online Services ISO Certification is available here: [ISO Certification](#)

(http://www.bsigroup.com/en/Assessment-and-certification-services/Client-directory/Search_Term: Microsoft Online Services)

Microsoft's Response (continued):

All Microsoft Online Services employees represent that they have reviewed, and agree to adhere to, all policies within the Information Security Policy documents.

All Microsoft Online Services Contractor Staff agree to adhere to the relevant policies within the Information Security Policy. Should one of these parties not have access to this policy for any reason, the supervising Microsoft agent is responsible for distributing the policy to them. A customer-facing version of the Information Security Policy can be made available upon request. Customers and prospective customers must have a signed NDA or equivalent in order to receive a copy of the Information Security Policy.

"Management Commitment to Information Security" and "Management Responsibility" is covered under the ISO 27001 standards, specifically addressed in Clause 5 and Annex A, domain 6.1.1. For more information review of the publicly available ISO standards we are certified against is suggested.'

Instructions for more information and guidance:

A review of the ISO 27001 and ISO 27002 publicly available standards is highly recommended. ISO Standards are available for purchase at the International Organization for Standardization website: http://www.iso.org/iso/iso_catalogue. These ISO standards provide deep detail and guidance. Once again the fact that Microsoft Online Services is certified to ISO 27001 means that we have met an external auditor's expectation that our environment achieves or exceeds such standards.

Example:

When reviewing the standard, one can take the ISO 27001 control or clause, and review specifics, e.g. “Management Commitment to Information Security” clause 5, from the ISO 27001 standard or the ISO 27002 advisory control 6.1.1 details:

ISO27002 (ISO 27002) (Download)



ISO27002 ISO 27002 Code of Practice for ISM PDF.

ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.

ISO/IEC 17799:2005 has now been renumbered ISO/IEC 27002:2005 (Information technology - Security techniques - Code of practice for information security management) . Both ISO/IEC 17799:2005 and ISO/IEC 27002:2005 are identical.

The standard details a comprehensive set of information security control objectives and a selection of best-practice controls.

Note: Due to our distribution relationship with ANSI, we are now able to offer the electronic PDF version of this standard at a much lower price than the hardcopy version - see the [press release](#).

Publisher: **ANSI/INCITS**

Format: **Electronic Download .PDF**

Licensing Terms: **Purchase and Use of this Product is Subject to this EULA**

Other formats: **ISMS 3 Standards Kit - (Download)**

Availability: **Immediate Download.**

“Management responsibility.....”

ISO27001 (ISO 27001) ISMS Requirements (PDF)



ISO27001 ISO 27001 ISO/IEC 27001 ISMS Requirements

ISO/IEC 27001 (Information technology - Security techniques - Information Security Management Systems - Requirements).

ISO/IEC 27001 is THE international information security management system standard against which an ISMS can be certified. Enabling organizations to meet all their information security-related regulatory compliance requirements (such as FISMA, GLBA, PIPEDA, etc), it is also closely allied with the Code of Practice ISO/IEC 27002 (formerly ISO/IEC17799).

An ISO/IEC 27001 compliant system will provide a systematic approach to ensuring the availability, confidentiality and integrity of corporate information. Using controls based on indentifying and combating the entire range of potential risks to the organization's information assets.

The standard draws on the expertise and knowledge of experienced information security practitioners in a wide range of significant organizations across more than 40 countries, to set out the best practice in information security. And is increasingly used by firms to demonstrate regulatory compliance and effective business risk management, as well as helping them to prepare and position themselves for all new and emerging regulations.

Resources

Visit our [Trust Center](#) and get:

- White papers
- Frequently Asked Questions
- Certification Information
- ISO Standards Available for Purchase

(Trust Center link: <http://go.microsoft.com/fwlink/?LinkID=206613&CLCID=0x409>)

The public copy of the Microsoft Online Services ISO Certification is available here:

[ISO Certification](http://www.bsigroup.com/en/Assessment-and-certification-services/Client-directory/Search_Term:Microsoft%20Online%20Services) ([http://www.bsigroup.com/en/Assessment-and-certification-services/Client-directory/Search_Term: Microsoft Online Services](http://www.bsigroup.com/en/Assessment-and-certification-services/Client-directory/Search_Term:Microsoft Online Services))

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls CO-01 through CO-02

Control ID In CCM ¹	Description (CCM Version R1.1. Final)	Microsoft Response
<p>CO-01 Compliance - Audit Planning</p>	<p>Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.</p>	<p>Our goals are to operate our services with security as a key principle, and to give you accurate assurances about our security. We have implemented and will maintain reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction. Each year, we undergo third-party audits by internationally recognized auditors to validate that we have independent attestation of compliance with our policies and procedures for security, privacy, continuity and compliance. Audit information is available under NDA upon request by prospective customers and through the Trust Center for current customers.</p> <p>Microsoft Online Services independent audit reports and certifications are shared with customers in lieu of individual customer audits. These certifications and attestations accurately represent how we obtain and meet our security and compliance objectives and serve as a practical mechanism to validate our promises for all customers.</p> <p>For security and operational reasons, Microsoft Online Services does not allow our customers to perform their own audits.</p> <p>“Monitor and review the Information Security Management System (ISMS)” is covered under the ISO 27001 standards, specifically addressed in Clause 4.2.3. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>CO-02 Compliance - Independent Audits</p>	<p>Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)</p>	<p>For more information see CO-01 or the Trust Center for our current certifications and third party attestations.</p>

¹ CCM content in columns 1 and 2 is © 2011 Cloud Security Alliance, used with permission.

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls CO-03 through CO-05

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>CO-03 Compliance - Third Party Audits</p>	<p>Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements.</p>	<p>Microsoft Online Services contractually requires third party service providers to Microsoft to maintain and meet requirements set forth in the Microsoft Online Services Information Security Policy. In addition, Microsoft Online Services requires that these third parties undergo an annual third party audit or arrange to be included in Microsoft Online Services annual third party audit.</p> <p>“Addressing security in third party agreements and third party service delivery management” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 6.2. and 10.2. For more information a review of the publicly available ISO standards we are certified against is suggested.</p>
<p>CO-04 Compliance - Contact / Authority Maintenance</p>	<p>Liaisons and points of contact with local authorities shall be maintained in accordance with business and customer requirements and compliance with legislative, regulatory, and contractual requirements. Data, objects, applications, infrastructure and hardware may be assigned legislative domain and jurisdiction to facilitate proper compliance points of contact.</p>	<p>Microsoft Online Services maintains contacts with external parties such as regulatory bodies, service providers, Risk Management organizations, and industry forums to ensure appropriate action can be quickly taken and advice obtained when necessary. Microsoft has a dedicated team for most contacts with law enforcement. Roles and responsibilities for managing and maintaining these relationships are defined.</p> <p>“Contact with authorities and contact with special interest groups” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 6.1.6 and 6.1.7. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>CO-05 Compliance - Information System Regulatory Mapping</p>	<p>Statutory, regulatory, and contractual requirements shall be defined for all elements of the information system. The organization's approach to meet known requirements, and adapt to new mandates shall be explicitly defined, documented, and kept up to date for each information system element in the organization. Information system elements may include data, objects, applications, infrastructure and hardware. Each element may be assigned a legislative domain and jurisdiction to facilitate proper compliance mapping.</p>	<p>Microsoft Online Services provides information about statutes and regulations it adheres to through its contract and service description, including by jurisdiction. Microsoft Online Services has an established process for identifying and implementing changes to services in response to changes in applicable statutes and regulations. Reviewed annually during our ISO 27001 audit. In addition, Microsoft Online Services web interface limits the ability to add users in jurisdictions that are outside of Microsoft Online Services scope of support.</p> <p>“Establish the ISMS, management review of the ISMS and compliance with legal requirements” is covered under the ISO 27001 standards, specifically addressed in Clauses 4.2.1 and 7.3 as well as in Annex A, domain 15.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Control CO-06

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>CO-06 Compliance - Intellectual Property</p>	<p>Policy, process and procedure shall be established and implemented to safeguard intellectual property and the use of proprietary software within the legislative jurisdiction and contractual constraints governing the organization.</p>	<p>All employees and contingent staff are required to follow applicable intellectual property laws and Microsoft maintains responsibility for use of proprietary software within the legislative jurisdictions and contractual constraints governing the organization. Prior to service readiness, each service undergoes a review of all third party software to ensure that it is properly licensed.</p> <p>In addition, Microsoft Online Services has policies and procedures to ensure adherence to the Digital Millennium Copyright Act “takedown” requirements as well as similar legislation on the service.</p> <p>Microsoft Online Services uses customer data only to maintain and provide Microsoft Online Services. Microsoft’s business services are designed separate from Microsoft’s consumer services. While some data may be stored or processed on systems used both for consumer and business services, business services data is not shared with systems used for advertising.</p> <p>“Establish the ISMS” is covered under the ISO 27001 standards, specifically addressed in Clause 4.2.1 for more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls DG-01 through DG-02

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>DG-01</p> <p>Data Governance - Ownership / Stewardship</p>	<p>All data shall be designated with stewardship with assigned responsibilities defined, documented and communicated.</p>	<p>Microsoft Online Services has implemented a formal policy that requires assets (the definition of asset includes data and hardware) used to provide Microsoft Online Services to be accounted for and have a designated asset owner. Asset owners are responsible for maintaining up-to-date information regarding their assets.</p> <p>“Allocation of information security responsibilities and ownership of assets” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 6.1.3 and 7.1.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>DG-02</p> <p>Data Governance - Classification</p>	<p>Data, and objects containing data, shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization and third party obligation for retention and prevention of unauthorized disclosure or misuse.</p>	<p>Microsoft Online Services standards provide guidance for classifying assets of several applicable security classification categories, and then implements a standard set of Security and privacy attributes.</p> <p>“Information classification” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 7.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls DG-03 through DG-04

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>DG-03</p> <p>Data Governance - Handling / Labeling / Security Policy</p>	<p>Policies and procedures shall be established for 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.</p>	<p>Microsoft Online Services standards provide guidance for classifying assets of several applicable security classification categories, and then implements a standard set of Security and privacy attributes.</p> <p>“Information classification, labeling and handling” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 7.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>DG-04</p> <p>Data Governance - Retention Policy</p>	<p>Policies and procedures for data retention and storage shall be established and backup or redundancy mechanisms implemented to ensure compliance with regulatory, statutory, contractual or business requirements. Testing the recovery of disk or tape backups must be implemented at planned intervals.</p>	<p>Microsoft Online Services provides capabilities for customers to apply data retention policies as defined in the individual service descriptions (http://www.microsoft.com/download/en/details.aspx?id=18459). As for backups, content is replicated from a primary data center to a secondary data center. As such, there is not a specific backup schedule as the replication is constant. Customers can choose to perform their own extractions/backups if necessary. Customer data is stored in a redundant environment with robust backup, restore, and failover capabilities to enable availability, business continuity, and rapid recovery. Multiple levels of data redundancy are implemented, ranging from redundant disks to guard against local disk failure to continuous, full data replication to a geographically dispersed data center. Microsoft online undergoes an annual validation of backup/recovery practices.</p> <p>“Information back-up” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.5.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls DG-05 through DG-06

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>DG-05</p> <p>Data Governance - Secure Disposal</p>	<p>Policies and procedures shall be established and mechanisms implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.</p>	<p>Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 compliant. For hard drives that can't be wiped we use a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained.</p> <p>All Microsoft Online Services utilize approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle.</p> <p>“Secure disposal or re-use of equipment and disposal of media” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 9.2.6 and 10.7.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>DG-06</p> <p>Data Governance - Non-Production Data</p>	<p>Production data shall not be replicated or used in non-production environments.</p>	<p>Microsoft applies the segregation of duty principle to ensure that access to test and production environments are restricted according to policy.</p> <p>Movement or copying of non-public customer data out of the production environment into a non-production environment is expressly prohibited except where customer consent is obtained, or at the directive of Microsoft's legal department.</p> <p>“Separation of development, test and operation facilities and protection of system test data” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 10.1.4 and 12.4.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls DG-07 through DG-08

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>DG-07</p> <p>Data Governance - Information Leakage</p>	<p>Security mechanisms shall be implemented to prevent data leakage.</p>	<p>Logical and physical controls are implemented in Microsoft Online Service's environments (see Office365 Security Service Description available through the Download Center), customers may elect to enhance the base capabilities through support for technology such as :</p> <ol style="list-style-type: none"> 1) Configuration of Message transport rules 2) Integration with Email data leakage protection products 3) Support for Integration of Active Directory rights Management Services 4) Exchange Hosted Encryption and alternative encryption products 5) SharePoint Online administrators can enable group or role based access control, built – in content auditing, and also can request admin access reports (via Customer Support Services) <p>“Information leakage” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 12.5.4. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>DG-08</p> <p>Data Governance - Risk Assessments</p>	<p>Risk assessments associated with data governance requirements shall be conducted at planned intervals considering the following:</p> <ul style="list-style-type: none"> • 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 	<p>Microsoft Online Services performs an annual business impact analysis. The analysis includes:</p> <ul style="list-style-type: none"> • The identification of threats relevant to the Microsoft Online Services business environment and process. • An assessment of the identified threats including potential impact and expected damage. • A management endorsed strategy for the mitigation of significant threats identified, and for the recovery of critical business processes. <p>“Establish the ISMS and Information classification and asset management” is covered under the ISO 27001 standards, specifically addressed in Clause 4.2.1 and Annex A, domain 7.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls FS-01 through FS-02

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>FS-01</p> <p>Facility Security - Policy</p>	<p>Policies and procedures shall be established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas.</p>	<p>Access to all 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 Data Centers. Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards. All guests are required to wear guest badges and be escorted by authorized Microsoft personnel.</p> <p>“Securing offices, rooms, and facilities” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9.1.3. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>FS-02</p> <p>Facility Security - User Access</p>	<p>Physical access to information assets and functions by users and support personnel shall be restricted.</p>	<p>Access is restricted by job function so that only essential personnel receive authorization to manage customers’ applications and services. Physical access authorization utilizes multiple authentication and security processes: badge and smartcard, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication for physical access to the data center environment.</p> <p>In addition to the physical entry controls that are installed on various doors within the data center, the Microsoft Data Center Management organization has implemented operational procedures to restrict physical access to authorized employees, contractors and visitors:</p> <ul style="list-style-type: none"> • Authorization to grant temporary or permanent access to Microsoft data centers is limited to authorized staff. The requests and corresponding authorization decisions are tracked using a ticketing/access system. • Badges are issued to personnel requiring access after verification of identification. • The Microsoft Data Center Management organization performs a regular access list review. As a result of this audit, the appropriate actions are taken after the review. <p>“Physical and environmental security” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls FS-03 through FS-05

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>FS-03</p> <p>Facility Security - Controlled Access Points</p>	<p>Physical security perimeters (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.</p>	<p>The data center buildings are nondescript and do not advertise that Microsoft Data Center hosting services are provided at the location. Access to the data center facilities is restricted. The main interior or reception areas have electronic card access control devices on the perimeter door(s), which restrict access to the interior facilities. Rooms within the Microsoft Data Center that contain critical systems (servers, generators, electrical panels, network equipment, etc.) are either restricted through various security mechanisms such as electronic card access control, keyed lock, ant tailgating and/or biometric devices. Additional physical barriers, such as “locked cabinets” or locked cages erected internal to facility perimeters, may be in place as required for certain assets according to Policy and/or by business requirement.</p> <p>“Physical security perimeter and environmental security” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>FS-04</p> <p>Facility Security - Secure Area Authorization</p>	<p>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.</p>	<p>“Public access, delivery, loading area and physical/environmental security” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9. For more information review of the publicly available ISO standards we are certified against is suggested.</p> <p>For additional information also see FS-03</p>
<p>FS-05</p> <p>Facility Security - Unauthorized Persons Entry</p>	<p>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.</p>	<p>“Public access, delivery, loading area and physical/environmental security” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9. For more information review of the publicly available ISO standards we are certified against is suggested.</p> <p>For additional information also see FS-03</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls FS-06 through FS-08

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
FS-06 Facility Security - Off-Site Authorization	Authorization must be obtained prior to relocation or transfer of hardware, software or data to an offsite premises.	<p>Microsoft Online Services asset and data protection procedures provide prescriptive guidance around the protection of logical and physical data and include instructions addressing relocation.</p> <p>“Removal of Property and change management” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 9.2.7 and 10.1.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
FS-07 Facility Security - Off-Site Equipment	Policies and procedures shall be established for securing and asset management for the use and secure disposal of equipment maintained and used outside the organization's premise.	<p>Microsoft's asset management policy and acceptable use standards was developed and implemented for Microsoft Online Services technology assets, infrastructure components and services technologies.</p> <p>A customer facing version of the Information Security Policy can be made available upon request. Customers and prospective customers must have a signed NDA or equivalent in order to receive a copy of the Information Security Policy.</p> <p>“Security of equipment off-premises” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9.2.5. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
FS-08 Facility Security - Asset Management	A complete inventory of critical assets shall be maintained with ownership defined and documented.	<p>Microsoft Online Services has implemented a formal policy that requires assets used to provide Microsoft Online Services to be accounted for and have a designated asset owner. An inventory of major hardware assets in the Microsoft Online Services environment is maintained. Asset owners are responsible for maintaining up-to-date information regarding their assets within the asset inventory including owner or any associated agent, location, and security classification. Asset owners are also responsible for classifying and maintaining the protection of their assets in accordance with the standards. Regular audits occur to verify inventory.</p> <p>“Asset management” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 7. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls HR-01 through HR-03

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>HR-01</p> <p>Human Resources Security - Background Screening</p>	<p>Pursuant to local laws, regulations, ethics and contractual constraints all employment candidates, contractors and third parties will be subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk.</p>	<p>All Microsoft US-based full-time employees (FTE), 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.</p> <p>Subcontractors who have access to non-public customer data may also be customer data are also required to successfully complete a background check prior to receiving access to customer data.</p> <p>Additional information and background checks, may also apply if the request for access relates to the federal environment. To protect the privacy of its employees, Microsoft does not share the results of background checks with customers. The screening process is owned by Microsoft Corporate Human Resources division.</p>
<p>HR-02</p> <p>Human Resources Security - Employment Agreements</p>	<p>Prior to granting individuals physical or logical access to facilities, systems or data employees, contractors, third party users and customers shall contractually agree and sign the terms and conditions of their employment or service contract, which must explicitly include the parties responsibility for information security.</p>	<p>All appropriate Microsoft employees take part in a Microsoft Online Services sponsored security-training program, and 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. Microsoft also has Non- Disclosure agreements built into our employee contracts.</p> <p>All Microsoft Online Services Contractor staff is required to take any training determined to be appropriate to the services being provided and the role they perform.</p> <p>"Roles and responsibilities as well as information security awareness, education and training" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 8. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>HR-03</p> <p>HR- Employee Termination</p>	<p>Roles and responsibilities for following performing employment termination or change in employment procedures shall be assigned, documented and communicated.</p>	<p>Microsoft Corporate Human Resources Policy drives employee termination processes.</p> <p>We do not create customer accounts; the customer creates the accounts either directly in Microsoft Online Services Portal, or in their local Active Directory, where the accounts can then be synchronized into Microsoft's Online Services. For this reason, the customer remains responsible for the accuracy of the user accounts they created.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls IS-01 through IS-02

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>IS-01</p> <p>Information Security - Management Program</p>	<p>An Information Security Management Program (ISMP) has been 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 should address, but not be limited to, the following areas insofar as they relate to the characteristics of the business:</p> <ul style="list-style-type: none"> • 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 	<p>An overall ISMS for Microsoft Online Services has been designed and implemented to address industry best practices around security, privacy and risk.</p> <p>A customer facing version of the Information Security Policy can be made available upon request. Customers and prospective customers must have a signed NDA or equivalent in order to receive a copy of the Information Security Policy.</p> <p>“Establishing and managing the ISMS and Organization of information security” is covered under the ISO 27001 standards, specifically addressed in Clause 4.2 and Annex A, domain 6. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-02</p> <p>Information Security - Management Support / Involvement</p>	<p>Executive and line management shall take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution</p>	<p>Each management-endorsed version of the Information Security Policy and all subsequent updates are distributed to all relevant stakeholders. The Information Security Policy is made available to all new and existing Microsoft Online Services employees for review. All Microsoft Online Services employees represent that they have reviewed, and agree to adhere to, all policies within the Information Security Policy documents. All Microsoft Online Services Contractor Staff agree to adhere to the relevant policies within the Information Security Policy. Should one of these parties not have access to this policy for any reason, the supervising Microsoft agent is responsible for distributing the policy to them.</p> <p>A customer facing version of the Information Security Policy can be made available upon request. Customers and prospective customers must have a signed NDA or equivalent in order to receive a copy of the Information Security Policy.</p> <p>“Management commitment to information security and management responsibility” is covered under the ISO 27001 standards, specifically addressed in Clause 5 and Annex A, domain 6.1.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Control IS-03 through IS-06

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>IS-03</p> <p>Information Security - Policy</p>	<p>Management shall approve a formal information security policy document which shall be communicated and published to employees, contractors and other relevant external parties. The Information Security Policy shall establish the direction of the organization and align to best practices, regulatory, federal/state and international laws where applicable. The Information Security policy shall be supported by a strategic plan and a security program with well-defined roles and responsibilities for leadership and officer roles.</p>	<p>Information security policy document is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 5.1.1, for more information review of the publicly available ISO standards we are certified against is suggested.</p> <p>For more information see IS-02</p>
<p>IS-04</p> <p>Information Security - Baseline Requirements</p>	<p>Baseline security requirements shall be established and applied to the design and implementation of (developed or purchased) applications, databases, systems, and network infrastructure and information processing that comply with policies, standards and applicable regulatory requirements. Compliance with security baseline requirements must be reassessed at least annually or upon significant changes.</p>	<p>As part of the overall ISMS framework baseline security requirements are constantly being reviewed, improved and implemented.</p> <p>“Information systems acquisition, development maintenance and security requirements of information systems” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 12. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-05</p> <p>Information Security - Policy Reviews</p>	<p>Management shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing effectiveness and accuracy.</p>	<p>The Microsoft Online Services Information Security Policy undergoes a formal review and update process at a regularly scheduled interval not to exceed 1 year. In the event a significant change is required in the security requirements, it may be reviewed and updated outside of the regular schedule.</p> <p>“Review of the information security policy” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 5.1.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-06</p> <p>Information Security - Policy Enforcement</p>	<p>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 stated as such in the policies and procedures.</p>	<p>Microsoft Online 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.</p> <p>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.</p> <p>Once a determination has been made that Microsoft Online Services Staff has violated Policy, Human Resources is informed, and is responsible for coordinating disciplinary response.</p> <p>“Information security awareness, education, training and disciplinary process” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 8.2.2 and 8.2.3. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls IS-07 through IS-08

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>IS-07</p> <p>Information Security - User Access Policy</p>	<p>User access policies and procedures shall be documented, approved and implemented for granting and revoking normal and privileged access to applications, databases, and server and network infrastructure in accordance with business, security, compliance and service level agreement (SLA) requirements.</p>	<p>Access control policy is a component of overall policies and undergoes a formal review and update process. Access to Microsoft Online Services' assets is granted based upon business requirements and with the asset owner's authorization. Additionally:</p> <ul style="list-style-type: none"> • Access to assets is granted based upon need-to-know and least-privilege principles. • Where feasible, 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. <p>"Access control" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-08</p> <p>Information Security - User Access Restriction / Authorization</p>	<p>Normal and privileged user access to applications, systems, databases, network configurations, and sensitive data and functions shall be restricted and approved by management prior to access granted.</p>	<p>Access control policy is a component of overall policies and undergoes a formal review and update process. Access to Microsoft Online Services' assets is granted based upon business requirements and with the asset owner's authorization. Additionally:</p> <ul style="list-style-type: none"> • Access to assets is granted based upon need-to-know and least-privilege principles. • Where feasible, 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. <p>"User access management and privilege management" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls IS-09 through IS-11

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>IS-09</p> <p>Information Security - User Access Revocation</p>	<p>Timely de-provisioning, revocation or modification of user access to the organizations systems, information assets and data shall be implemented upon any change in status of employees, contractors, customers, business partners or third parties. Any change in status is intended to include termination of employment, contract or agreement, change of employment or transfer within the organization.</p>	<p>Managers, owners of applications and data are responsible for reviewing who has access on a periodic basis. Regular access review audits occur to validate appropriate access provisioning has occurred.</p> <p>“Removal of access rights” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 8.3.3. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-10</p> <p>Information Security - User Access Reviews</p>	<p>All levels of user access shall be reviewed by management at planned intervals and documented. For access violations identified, remediation must follow documented access control policies and procedures.</p>	<p>Managers and owners of applications and data are responsible for reviewing who has access on a periodic basis. Microsoft Online provides enhanced capabilities to allow customers to audit and delegate end user access within the service offering, please review the corresponding service descriptions for details.</p> <p>“User access management and privilege management” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-11</p> <p>Information Security - Training / Awareness</p>	<p>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, process and policies, relating to their function relative to the organization.</p>	<p>All appropriate Microsoft Staff take part in a Microsoft Online Services sponsored security-training program, and 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. An example of an internal training is BlueHat.</p> <p>All Microsoft Online Services Contractor staff are required to take any training determined to be appropriate to the services being provided and the role they perform.</p> <p>“Information security awareness, education and training” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 8.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls IS-12 through IS-14

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>IS-12</p> <p>Information Security - Industry Knowledge / Benchmarking</p>	<p>Industry security knowledge and benchmarking through networking, specialist security forums, and professional associations shall be maintained.</p>	<p>Microsoft is a member of several industry organizations and both attends and provides speakers to such events and organizations. Microsoft additionally holds several internal trainings.</p> <p>“Contact with special interest groups” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 6.1.7. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-13</p> <p>Information Security - Roles/ Responsibilities</p>	<p>Roles and responsibilities of contractors, employees and third party users shall be documented as they relate to information assets and security.</p>	<p>The Microsoft Online Services Information Security Policy exists in order to provide Microsoft Online Services 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 the Microsoft Online Services. The Policy has been created as a component of an overall Information Security Management System (ISMS) for the Microsoft Online Services. The Policy has been reviewed, approved, and is endorsed by Microsoft Online Services management.</p> <p>“Roles and responsibilities of contractors, employees and third party users” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 8.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-14</p> <p>Information Security - Management Oversight</p>	<p>Managers are responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility.</p>	<p>Each management-endorsed version of the Policy and all subsequent updates are distributed to all relevant stakeholders. The Policy is made available to all new and existing Microsoft Online Services Staff for review. All Microsoft Online Services Staff represent that they have reviewed, and agree to adhere to, all policies within the Policy documents. All Microsoft Online Services Contractor Staff agree to adhere to the relevant policies within the Policy. Should one of these parties not have access to this policy for any reason, the supervising Microsoft agent is responsible for distributing the policy to them.</p> <p>“Management responsibility and management commitment to information security and responsibilities” is covered under the ISO 27001 standards, specifically addressed in Clause 5 and Annex A, domain 6.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls IS-15 through IS-17

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>IS-15</p> <p>Information Security - Segregation of Duties</p>	<p>Policies, process and procedures shall be implemented to enforce and assure proper segregation of duties. In those events where user-role conflict of interest constraint exists, technical controls shall be in place to mitigate any risks arising from unauthorized or unintentional modification or misuse of the organization's information assets.</p>	<p>Office 365 services can have distinct hosted services development and operations staff to adhere to the principle of segregation of duty. Access to source code, build servers, and the production environment is strictly controlled. For example:</p> <ul style="list-style-type: none"> • Access to the Office 365 services production environment is restricted to operations personnel. Development and test teams may be granted access to information provided from within the production environment to help troubleshoot issues. • Access to the Office 365 services source code control is restricted to engineering personnel; operations personnel cannot change source code. <p>Microsoft personnel build the servers before they are commissioned for the multi-tenant environment. Once a server build is complete, the build teams have their permissions removed. From the time of server commission, there are limited pathways through which Microsoft personnel may obtain permissions to a system running on the commissioned server. Support staff may obtain access as a direct result of a service ticket requiring access or an update to the system to install software or resolve a problem. In such cases, the audit log would show who logged in and when. The processes Office 365 uses comply with the certifications Microsoft maintains.</p> <p>Segregation of duties is implemented for sensitive and/or critical functions in Microsoft Online Services' environments in order to minimize the potential of fraud, misuse, or error</p> <p>"Segregation of duties" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.1.3. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-16</p> <p>Information Security - User Responsibility</p>	<p>Users shall be made aware of their responsibilities for:</p> <ul style="list-style-type: none"> • Maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements • Maintaining a safe and secure working environment • Leaving unattended equipment in a secure manner 	<p>All appropriate Office 365 employees take part in a Microsoft Online Services security-training program, and are recipients of periodic security awareness updates when applicable. Security education is an on-going process and is conducted at minimum annually in order to minimize risks.</p> <p>All Microsoft Online Services Contractor staff is required to take any training determined to be appropriate to the services being provided and the role they perform.</p> <p>"User responsibilities" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.3. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-17</p> <p>Information Security Workspace</p>	<p>Policies and procedures shall be established for clearing visible documents containing sensitive data when a workspace is unattended and enforcement of workstation session logout for a period of inactivity.</p>	<p>Technical and procedural controls are part of Microsoft's policies including areas such as defined session time-out requirements.</p> <p>"User responsibilities" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.3. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls IS-18 through IS-19

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>IS-18</p> <p>Information Security - Encryption</p>	<p>Policies and procedures shall be established and mechanisms implemented for encrypting sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging).</p>	<p>Encryption is provided on several layers, such as Transport Layer, encryption between clients and Exchange Online (SSL), Instant Messaging and IM federation. For more information consult the Office 365 Security Service Description available on the Download Center. Furthermore, we support S/MIME, Active Directory Rights Management Services or PGP.</p> <p>Office 365 currently does not encrypt data at rest, however, the customer may do so through IRM or RMS.</p> <p>“Exchange of information” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.8. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-19</p> <p>Information Security - Encryption Key Management</p>	<p>Policies and procedures shall be established and mechanisms implemented for effective key management to support encryption of data in storage and in transmission.</p>	<p>Encryption is provided on several layers, such as Transport Layer, encryption between clients and Exchange Online (SSL), Instant Messaging and IM federation. For more information consult the Office 365 Security Service Description available on the Download Center. Furthermore, we support S/MIME, Active Directory Rights Management Services or PGP.</p> <p>Office 365 currently does not encrypt data at rest, however, the customer may do so through IRM or RMS.</p> <p>“Media Handling” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.7.3. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Control IS-20

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p style="text-align: center;">IS-20</p> <p>Information Security - Vulnerability / Patch Management</p>	<p>Policies and procedures shall be established and mechanism implemented for vulnerability and patch management, ensuring that application, system, and network device vulnerabilities are evaluated and Contractor-supplied security patches applied in a timely manner taking a risk-based approach for prioritizing critical patches.</p>	<p>Microsoft Online Services implements technologies to scan the environment for vulnerabilities. Identified vulnerabilities are tracked, and verified for remediation. In addition, regular vulnerability/penetration assessments to identify vulnerabilities and determine whether key logical controls are operating effectively are performed.</p> <p>Microsoft's Security Response Center (MSRC) regularly monitors external security vulnerability awareness sites. As part of the routine vulnerability management process, Microsoft Online Services evaluates our exposure to these vulnerabilities and leads action across Microsoft Online Services to mitigate risks when necessary.</p> <p>The Microsoft Security Response Center (MSRC) releases security bulletins on the second Tuesday of every month ("Patch Tuesday"), or as appropriate to mitigate zero-day exploits. In the event that proof-of-concept code is publicly available regarding a possible exploit, or if a new critical security patch is released, Microsoft Online Services is required to apply patches to affected Microsoft Online Services systems according to a patching policy to remediate the vulnerability to the customer's hosted environment.</p> <p>"Control of technical vulnerabilities" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 12.6. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls IS-21 through IS-22

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>IS-21</p> <p>Information Security - Anti-Virus / Malicious Software</p>	<p>Ensure that all antivirus programs are capable of detecting, removing, and protecting against all known types of malicious or unauthorized software with antivirus signature updates at least every 12 hours.</p>	<p>Microsoft Online Services run multiple layers of anti-virus software to ensure protection from common malicious software. For example, servers within the Microsoft Online environment run anti-virus software that scans files uploaded and downloaded from the service for viruses. Additionally, Microsoft Exchange mail servers run additional anti-virus software that focuses on scanning email messages for malware. Additional information may be found in the relevant service descriptions and Service Level Agreement (SLA).</p> <p>Microsoft has its own Security Response Center (MSRC) that is also supplies information to all our customers covering the whole range Microsoft products. More information can be found on http://www.microsoft.com/security/msrc/default.aspx.</p> <p>“Protection against malicious code” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.4. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-22</p> <p>Information Security - Incident Management</p>	<p>Policy, process and procedures shall be established to triage security related events and ensure timely and thorough incident management.</p>	<p>Microsoft Online has developed robust processes to facilitate a coordinated response to incidents if one was to occur. A security incident may include, but are not limited to: e-mail viruses, malware, worms, denial of service attacks, unauthorized access, and any other type of unauthorized, or unlawful activity involving Microsoft Online computer networks or data processing equipment.</p> <p>Our process consists of the following steps: Identification, containment, eradication, recovery, and lessons learned.</p> <p>“Security incident response plans” are covered under the ISO 27001 standards, specifically addressed in Annex A, domain 13.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Control IS-23

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>IS-23 Information Security - Incident Reporting</p>	<p>Contractors, employees and third party users shall be made aware of their responsibility to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a prompt and expedient manner in compliance with statutory, regulatory and contractual requirements.</p>	<p>All Microsoft Online Services' security incidents, weaknesses, and malfunctions are required to be reported by Microsoft Online Services Staff and Contractor Staff immediately. The reporting and handling of these events follow prescribed procedures pursuant to defined and implemented policy.</p> <p>Microsoft Online has developed robust processes to facilitate a coordinated response to incidents if one was to occur. A security event may include, among other things unlawful access to customer data stored on our equipment and facilities and unauthorized access resulting in loss, disclosure or alteration of customer data.</p> <p>The Microsoft Online Security Incident Response process follows the following phases:</p> <ul style="list-style-type: none"> • Identification – System and security alerts may be harvested, correlated, and analyzed. Events are investigated by Microsoft Online operational and security organizations. . If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft. This escalation will include product, security, and engineering specialists. • Containment – The escalation team evaluates the scope and impact of an incident. The immediate priority of the escalation team is to ensure the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. In the case where in-depth investigation is required, content is collected from the subject systems using best-of-breed forensic software and industry best practices. • Eradication – After the situation is contained, the escalation team moves toward eradicating any damage caused by the security breach, and identifies the root cause for why the security issue occurred. If vulnerability is determined, the escalation team reports the issue to product engineering. • Recovery – During recovery, software or configuration updates are applied to the system and services are returned to a full working capacity. • Lessons Learned – Each security incident is analyzed to ensure the appropriate mitigations applied to protect against future reoccurrence. <p>“Reporting security weaknesses and responsibilities and procedures” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 13.1.2 and 13.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls IS-24 through IS-26

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>IS-24</p> <p>Information Security - Incident Response Legal Preparation</p>	<p>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 collection, retention, and presentation of evidence to support potential legal action subject to the relevant jurisdiction.</p>	<p>As part of the 'containment' step in our Security Incident Response Process, the immediate priority of the escalation team is to ensure the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. In the case where in-depth investigation is required, content is collected from the subject systems using best-of-breed forensic software and industry best practices.</p> <p>"Security incident response plans and collection of evidence" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 13.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-25</p> <p>Information Security - Incident Response Metrics</p>	<p>Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.</p>	<p>At the outset of an incident, the Risk Management organization evaluates incidents to assess their severity. This will be done in conjunction with representatives of the affected property or properties. An accurate estimate of the severity of an incident will guide the team in determining the breadth of its communications and formulation of a response strategy. The severity rating of an incident may change as additional information is revealed in an investigation. It is the responsibility of Security Incident Management personnel to update the rating and communicate changes to all stakeholders.</p> <p>"Management information security incidents and learning from information security incidents" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 13.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-26</p> <p>Information Security - Acceptable Use</p>	<p>Policies and procedures shall be established for the acceptable use of information assets.</p>	<p>The Product Use Rights Policy was developed and implemented to supplement Microsoft's acceptable use standard, with Microsoft Online Services specific acceptable use criteria. For Microsoft Online Services technology assets, infrastructure components and services technologies. The Product Use Rights is available online at: http://www.microsoft.com/licensing/pur/products.aspx</p> <p>"Acceptable use" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 7.1.3. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls IS-27 through IS-29

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>IS-27</p> <p>Information Security - Asset Returns</p>	<p>Employees, contractors and third party users must return all assets owned by the organization within a defined and documented time frame once the employment, contract or agreement has been terminated.</p>	<p>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.</p> <p>“Return of assets” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 8.3.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-28</p> <p>Information Security - eCommerce Transactions</p>	<p>Electronic commerce (e-commerce) related data traversing 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.</p>	<p>Office 365 is not an e-commerce solution. However, encryption is provided on several layers, such as Transport Layer, encryption between clients and Exchange Online (SSL), Instant Messaging and IM federation. For more information consult the Office 365 Security Service Description available on the Download Center. Furthermore, we support S/MIME, Active Directory Rights Management Services or PGP.</p>
<p>IS-29</p> <p>Information Security - Audit Tools Access</p>	<p>Access to, and use of, audit tools that interact with the organizations information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.</p>	<p>A delegated management model enables administrators to have only the access they need to perform specific tasks, reducing the potential for error and allowing access to systems and functions strictly on an as-needed basis. Microsoft Online Services has formal monitoring processes to include frequency of review for Standard Operating Procedures and review oversight processes and procedures</p> <p>“Protection of information systems audit tools and protection of log information” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 15.3.2 and 10.10.3 . For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls IS-30 through IS-31

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>IS-30</p> <p>Information Security - Diagnostic / Configuration Ports Access</p>	<p>User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.</p>	<p>Access control policy is a component of overall policies and undergoes a formal review and update process. Access to Microsoft Online Services' assets is granted based upon business requirements and with the asset owner's authorization. Additionally:</p> <ul style="list-style-type: none"> • Access to assets is granted based upon need-to-know and least-privilege principles. • Where feasible, 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. <p>Microsoft Online Services controls physical access to diagnostic and configuration ports through physical data center controls described and supporting procedures to control physical access to the port. Diagnostic and configuration ports are only accessible by arrangement between service/asset owner and hardware/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.</p> <p>"Network controls access controls" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.6.1, 11.1.1, and 11.4.4. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>IS-31</p> <p>Information Security - Network / Infrastructure Services</p>	<p>Network and infrastructure service level agreements (in-house or outsourced) shall clearly document security controls, capacity and service levels, and business or customer requirements.</p>	<p>Capacity management: 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. System performance and capacity utilization is proactively planned to optimize the environment.</p> <p>Security: The networks within the Office 365 data centers are designed to create multiple separate network segments within each data center. This segmentation helps to provide physical separation of critical, back-end servers and storage devices from the public-facing interfaces.</p> <p>"Addressing security in third party agreements and security of network services" is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 6.2.3 and 10.6.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls IS-32 through LG-01

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
IS-32 Information Security - Portable / Mobile Devices	<p>Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).</p>	<p>Mobile computing devices (i.e. Laptops, Smart Phones, etc...) are not permitted in, or directly attached to, any Microsoft Online Services production environment, unless those devices have been approved for use by Microsoft Online Services Management.</p> <p>Office 365 supports a range of mobile devices to access Office 365 service to customers. In such circumstances, the customer is responsible for adherence to their policies and adequate end-point protection.</p> <p>"Access control to mobile computing and communications" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.7.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
IS-33 Information Security - Source Code Access Restriction	<p>Access to application, program or object source code shall be restricted to authorized personnel on a need to know basis. Records shall be maintained regarding the individual granted access, reason for access and version of source code exposed.</p>	<p>Access to Microsoft Online Services' source code libraries is limited to authorized Microsoft Online Services Staff and Microsoft Online Services Contractors. Where feasible, source code libraries maintain separate project work spaces for independent projects. Microsoft Online Services Staff and Microsoft Online Services Contractor Staff are granted access only to those work spaces which they need access to perform their duties. An audit log detailing modifications to the source code library is maintained, and reviewed during regular audits.</p> <p>"Access control and access control to program source code" is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 11 and 12.4.3. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
IS-34 Information Security - Utility Programs Access	<p>Utility programs capable of potentially overriding system, object, network, virtual machine and application controls shall be restricted.</p>	<p>Active Directory has mechanisms to restrict access and log activities.</p> <p>"User authentication for external connections" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.4.2. For more information, review of the publicly available ISO standards we are certified against is suggested.</p>
LG-01 Legal - Non-Disclosure Agreements	<p>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.</p>	<p>Microsoft Legal and Human Resources maintain policies and procedures defining the implementation and execution of non-disclosure and confidentiality agreements.</p> <p>"Confidentiality agreements and non-disclosure agreements" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 6.1.5. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls LG-02 through OP-01

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>LG-02</p> <p>Legal - Third Party Agreements</p>	<p>Third party agreements that directly, or indirectly, impact the organizations information assets or data are required to include explicit coverage of all relevant security requirements. This includes agreements involving processing, accessing, communicating, hosting or managing the organization's information assets, or adding or terminating services or products to existing information. Assets agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.</p>	<p>Microsoft Online Services standards specify that the Microsoft Online Services Risk Management organization approves certain exchanges with parties outside of Microsoft Online Services. As part of this process, the Risk Management organization ensures that exchanges of High Business Impact(Loss could result in immediate, direct, considerable impact to business and includes Highly Sensitive Personally Identifiable Information) and Medium Business Impact(Loss could result in indirect, limited impact to the business and includes Personally Identifiable Information) assets with non-Microsoft parties are made only in connection with a formal procedure.</p> <p>“Addressing security in third party agreements” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 6.2.3. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>OP-01</p> <p>Operations Management - Policy</p>	<p>Policies and procedures shall be established and made available for all personnel to adequately support services operations role.</p>	<p>Consistent with Microsoft policy, hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities and tasks involved in the job, background characteristics needed to perform the job, and personal characteristics required. Once the requirements are determined, managers create a job description, which is a profile of the job and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and to make an appropriate hiring decision.</p> <p>“Information security policy” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 5.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls *OP-02 through OP-04*

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>OP-02</p> <p>Operations Management - Documentation</p>	<p>Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) shall be made available to authorized personnel to ensure the following:</p> <ul style="list-style-type: none"> • Configuring, installing, and operating the information system • Effectively using the system's security features 	<p>Standard Operating Procedures are formally documented and approved by Microsoft Online Services management. The standard operating procedures are reviewed at least once per year. Microsoft Online Services makes available comprehensive guidance, help, training and troubleshooting materials as part of the Office 365 Service. Within the Administration Portal, there are links to many of the resources available, including:-</p> <ul style="list-style-type: none"> • Help articles for Users, and administrators who need to Manage Office 365 • Videos for Exchange Administrators • Articles and steps required to configure hybrid environments • Community forums/wikis where help articles and whitepapers are published • Service Health Dashboard. For information regarding outages/issues <p>“Documented operating procedures and security of system documentation” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 10.1.1 and 10.7.4. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>OP-03</p> <p>Operations Management - Capacity / Resource Planning</p>	<p>The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with regulatory, contractual and business requirements. Projections of future capacity requirements shall be made to mitigate the risk of system overload.</p>	<p>Microsoft has the following operational processes in place: proactive capacity management based on defined thresholds or events; hardware and software subsystem monitoring for acceptable service performance and availability, CPU utilization, service utilization, storage utilization and network latency.</p> <p>“Capacity management” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.3.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>OP-04</p> <p>Operations Management - Equipment Maintenance</p>	<p>Policies and procedures shall be established for equipment maintenance ensuring continuity and availability of operations.</p>	<p>A process for the development and maintenance of a Services Continuity Management (SCM) is in place for the Microsoft Online Services' environment. The process contains a strategy for the recovery of Microsoft Online Services assets and the resumption of key Microsoft Online Services' business processes. The continuity solution reflects security, compliance and privacy requirements of the service production environment at the alternate site.</p> <p>“Equipment maintenance” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9.2.4. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls RI-01 through RI-03

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>RI-01</p> <p>Risk Management - Program</p>	<p>Organizations shall develop and maintain an enterprise risk management framework to manage risk to an acceptable level.</p>	<p>The ISO Plan, Do, Check, Act process is used by Microsoft Online Services to continually maintain and improve the risk management framework.</p> <p>“Establishing the ISMS and risk management framework” is covered under the ISO 27001 standards, specifically addressed in domain 4.2.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>RI-02</p> <p>Risk Management - Assessments</p>	<p>Aligned with the enterprise-wide framework. Formal risk assessments shall be performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).</p>	<p>Microsoft's Online Services Risk Management organization bases the risk assessment framework on the ISO27001 standards. An integrated part of the methodology is the Risk Assessment process. The Risk Assessment Assess phase begins with identifying risks, establishing a risk level by determining the likelihood of occurrence and impact, and finally, identifying controls and safeguards that reduce the impact of the risk to an acceptable level. According measures, recommendations and controls are put in place to mitigate the risks to the extent possible.</p> <p>“Establishing and managing the ISMS” is covered under the ISO 27001 standards, specifically addressed in Clause 4.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>RI-03</p> <p>Risk Management - Mitigation / Acceptance</p>	<p>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 executive approval.</p>	<p>Microsoft's Online Services Risk Management organization bases the risk assessment framework on the ISO27001 standards. An integrated part of the methodology is the Risk Assessment process.</p> <p>The Risk Assessment Assess phase begins with identifying risks, establishing a risk level by determining the likelihood of occurrence and impact, and finally, identifying controls and safeguards that reduce the impact of the risk to an acceptable level. According measures, recommendations and controls are put in place to mitigate the risks to the extent possible.</p> <p>“Establishing and managing the ISMS” is covered under the ISO 27001 standards, specifically addressed in Clause 4.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls RI-04 through RI-05

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>RI-04</p> <p>Risk Management - Business / Policy Change Impacts</p>	<p>Risk assessment results shall include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective.</p>	<p>Decisions to update policies and procedures are based on the risk assessment reports. Risk Assessments are regularly reviewed based on periodicity and changes emerging to the risk landscape.</p> <p>“Establishing the ISMS and risk management framework” is covered under the ISO 27001 standards, specifically addressed in Clause 4.2.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>RI-05</p> <p>Risk Management - Third Party Access</p>	<p>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.</p>	<p>Access control policy is a component of overall policies and undergoes a formal review and update process. Access to Microsoft Online Services' assets is granted based upon business requirements and with the asset owner's authorization. Additionally:</p> <ul style="list-style-type: none"> • Access to assets is granted based upon need-to-know and least-privilege principles. • Where feasible, 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. <p>“Identification of risks related to external parties and access control” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 6.2.1 and 11. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls RM-01 through RM-02

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>RM-01</p> <p>Release Management - New Development / Acquisition</p>	<p>Policies and procedures shall be established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities.</p>	<p>An operational change control procedure is in place for Microsoft Online Services and system changes. This procedure includes a process for Microsoft Online Services management review and approval. This change control procedure is communicated to all parties (Microsoft Online Services and third parties) who perform system maintenance on, or in, any of the Microsoft Online Services facilities. The operational change control procedure considers the following actions:</p> <ul style="list-style-type: none"> • The identification and documentation of the planned change • An assessment process of possible change impact • Change testing in an approved non-production environment • Change communication plan • Change management approval process • Change abort and recovery plan (when applicable) <p>Customers will be given 12 months' notice of disruptive changes and a minimum of 5 days' notice for planned maintenance; however, due to the multi-tenancy nature of the service there are no provisions to allow individual customers to define when upgrades can occur.</p> <p>"Change management" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.1.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>RM-02</p> <p>Release Management - Production Changes</p>	<p>Changes to the production environment shall be documented, tested and approved prior to implementation. Production software and hardware changes may include applications, systems, databases and network devices requiring patches, service packs, and other updates and modifications.</p>	<p>For more information see RM -01.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls RM-03 through RM-05

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>RM-03</p> <p>Release Management - Quality Testing</p>	<p>A program for the systematic monitoring and evaluation to ensure that standards of quality are being met shall be established for all software developed by the organization. Quality evaluation and acceptance criteria for information systems, upgrades, and new versions shall be established, documented and tests of the system(s) shall be carried out both during development and prior to acceptance to maintain security. Management shall have a clear oversight capacity in the quality testing process with the final product being certified as "fit for purpose" (the product should be suitable for the intended purpose) and "right first time" (mistakes should be eliminated) prior to release.</p>	<p>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 Security Development Lifecycle is at the core of Microsoft Online Services. For more information visit: http://www.microsoft.com/security/sdl/.</p> <p>"Security in development and support processes" is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 12.5. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>RM-04</p> <p>Release Management - Outsourced Development</p>	<p>A program for the systematic monitoring and evaluation to ensure that standards of quality are being met shall be established for all outsourced software development. The development of all outsourced software shall be supervised and monitored by the organization and must include security requirements, independent security review of the outsourced environment by a certified individual, certified security training for outsourced software developers, and code reviews. Certification for the purposes of this control shall be defined as either an ISO/IEC 17024 accredited certification or a legally recognized license or certification in the legislative jurisdiction the organization outsourcing the development has chosen as its domicile.</p>	<p>Microsoft applies Security Development Lifecycle, a software security assurance process, to design, develop, and implement Office 365 services. Security Development Lifecycle helps to ensure that communication and collaboration services are highly secured—even at the foundation level. Through controls like Establish Design Requirements, Analyze Attack Surface, and Threat Modeling, Security Development Lifecycle helps Microsoft identify: Potential threats while running a service, Exposed aspects of the service that are open to attack.</p> <p>If potential threats are identified at Design, Development, or Implementation phases, Microsoft can minimize the probability of attacks by restricting services or eliminating unnecessary functions. After eliminating the unnecessary functions, Microsoft reduces these potential threats in the Verification phase by fully testing the controls in the Design phase. More information can be found in: http://www.microsoft.com/security/sdl/</p> <p>"Security in development and support processes" is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 12.5. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>RM-05</p> <p>Release Management - Unauthorized Software Installations</p>	<p>Policies and procedures shall be established and mechanisms implemented to restrict the installation of unauthorized software.</p>	<p>All changes into production are going through the Change Management process described in RM-01. All code is explicitly installed on our servers by Administrators through the change control process.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls RS-01 through R1-02

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>RS-01</p> <p>Resiliency - Management Program</p>	<p>Policy, process and procedures defining business continuity and disaster recovery shall be put in place to minimize the impact of a realized risk event on the organization to an acceptable level and facilitate recovery of information assets (which may be the result of. For example, natural disasters, accidents, equipment failures, and deliberate actions) through a combination of preventive and recovery controls, in accordance with regulatory, statutory, contractual, and business requirements and consistent with industry standards. This Resiliency management program shall be communicated to all organizational participants with a need to know basis prior to adoption and shall also be published, hosted, stored, recorded and disseminated to multiple facilities which must be accessible in the event of an incident.</p>	<p>A process for the development and maintenance of a Services Continuity Management (SCM) is in place for the Microsoft Online Services' environment. The process contains a strategy for the recovery of Microsoft Online Services assets and the resumption of key Microsoft Online Services' business processes. The continuity solution reflects security, compliance and privacy requirements of the service production environment at the alternate site.</p> <p>"Information security aspects of business continuity management" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 14.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>RS-02</p> <p>Resiliency - Impact Analysis</p>	<p>There shall be a defined and documented method for determining the impact of any disruption to the organization which must incorporate the following:</p> <ul style="list-style-type: none"> • 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 services within their maximum tolerable period of disruption • Estimate the resources required for resumption 	<p>A business impact analysis is performed and reviewed at appropriate intervals. The analysis includes:</p> <ul style="list-style-type: none"> • The identification of threats relevant to the Microsoft Online Services business environment and process. • An assessment of the identified threats including potential impact and expected damage. • A management endorsed strategy for the mitigation of significant threats identified, and for the recovery of critical business processes <p>"Information security aspects of business continuity management" is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 14.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls RS-03 through R1-05

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>RS-03</p> <p>Resiliency - Business Continuity Planning</p>	<p>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 and maintenance and information security requirements. Requirements for business continuity plans include the following:</p> <ul style="list-style-type: none"> • 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 	<p>Microsoft Online Services maintains a framework that is consistent with industry and Microsoft best practices that drives the continuity program at all levels. The Microsoft Online Services framework includes:</p> <ul style="list-style-type: none"> • Assignment of key resource responsibilities • Notification, escalation and declaration processes • Recovery Time Objectives and Recovery Point Objectives • Continuity plans with documented procedures • Training program for preparing all appropriate parties to execute the Continuity Plan • A testing, maintenance, and revision process <p>“Information security aspects of business continuity management” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 14.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>RS-04</p> <p>Resiliency - Business Continuity Testing</p>	<p>Business continuity plans shall be subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness.</p>	<p>Recovery plans are validated on a regular basis per industry best practices to ensure that solutions are viable at time of event.</p> <p>“Testing, maintaining and re-assessing business continuity plans” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 14.1.5. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>RS-05</p> <p>Resiliency - Environmental Risks</p>	<p>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, earthquake, tsunami, explosion, nuclear mishap, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed and countermeasures applied.</p>	<p>Environmental controls have been implemented to protect the data center including:</p> <ul style="list-style-type: none"> • Temperature control • Heating, Ventilation and Air Conditioning (HVAC) • Fire detection and suppression systems • Power Management systems <p>“Protecting against external and environmental threats” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9.1.4. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls RS-06 through R1-08

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>RS-06</p> <p>Resiliency - Equipment Location</p>	<p>To reduce the risks from environmental threats, hazards and opportunities for unauthorized access equipment shall be located away from locations subject to high probability environmental risks and supplemented by redundant equipment located a reasonable distance.</p>	<p>Microsoft Online Services' equipment is placed in environments which have been engineered to be protective from theft and environmental risks such as fire, smoke, water, dust, vibration, earthquake, and electrical interference.</p> <p>“Protecting against external and environmental threats and equipment siting protection” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 9.1.4 and 9.2.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>RS-07</p> <p>Resiliency - Equipment Power Failures</p>	<p>Security mechanisms and redundancies shall be implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.).</p>	<p>The data centers have dedicated 24x7 uninterruptible power supply (UPS) and emergency power support, i.e. generators. Regular maintenance and testing is conducted for both the UPS and generators. Data centers have made arrangements for emergency fuel delivery.</p> <p>The data center has a dedicated Facility Operations Center to monitor the following:</p> <ul style="list-style-type: none"> • Power systems, including all critical electrical components – generators, transfer switch, main switchgear, power management module and uninterruptible power supply equipment. • The Heating, Ventilation and Air Conditioning (HVAC) system, which controls and monitors space temperature and humidity within the data centers, space pressurization and outside air intake. <p>Fire Detection and Suppression systems exist at all data centers.</p> <p>Additionally, portable fire extinguishers are available at various locations in the data center. Routine maintenance is performed on facility and environmental protection equipment.</p> <p>“Protecting against external and environmental threats and supporting utilities” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 9.1.4 and 9.2.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>RS-08</p> <p>Resiliency - Power / Telecommunications</p>	<p>Telecommunications equipment, cabling and relays transecting data or supporting services shall be protected from interception or damage and designed with redundancies, alternative power source and alternative routing.</p>	<p>“Cabling security and supporting utilities” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 9.2.3 and 9.2.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p> <p>For more information see RS-07</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix

Control SA-01

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>SA-01</p> <p>Security Architecture - Customer Access Requirements</p>	<p>Prior to granting customers access to data, assets and information systems, all identified security, contractual and regulatory requirements for customer access shall be addressed and remediated.</p>	<p>Our customers around the world are subject to many different laws and regulations. Legal requirements in one country or industry may be inconsistent with legal requirements applicable elsewhere. As a provider of global cloud services, we must run our services with common operational practices and features across multiple customers and jurisdictions. To help our customers comply with their own requirements, we build our services with common privacy and security requirements in mind. To the extent that we identified security, contractual and regulatory work to the customer that we will be requiring of ourselves we have addressed and remediated these requirements through a set regime of testing prior to sale of services and ongoing thereafter. However, it is ultimately up to our customers to evaluate our offerings against their own requirements, so they can determine if our services satisfy their regulatory needs. We are committed to providing our customers detailed information about our cloud services to help them make their own regulatory assessments.</p> <p>“Identification of risks related to external parties and access control policy” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 6.2.1 and 11.1.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix

Control SA-02

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>SA-02</p> <p>Security Architecture - User ID Credentials</p>	<p>Implement and enforce (through automation) user credential and password controls for applications, databases and server and network infrastructure, requiring the following minimum standards:</p> <ul style="list-style-type: none"> • User identity verification prior to password resets. • If password reset initiated by personnel other than user (i.e., administrator), password must be immediately changed by user upon first use. • Timely access revocation for terminated users. • Remove/disable inactive user accounts at least every 90 days. • Unique user IDs and disallow group, shared, or generic accounts and passwords. • Password expiration at least every 90 days. • Minimum password length of at least seven (7) characters. • Strong passwords containing both numeric and alphabetic characters. • Allow password re-use after the last four (4) passwords used. • User ID lockout after not more than six (6) attempts. • User ID lockout duration to a minimum of 30 minutes or until administrator enables the user ID. • Re-enter password to reactivate terminal after session idle time for more than 15 minutes. • Maintain user activity logs for privileged access. 	<p>Microsoft Online Services uses Active Directory to manage enforcement of our password policy. Microsoft Online Services systems are configured to force users to use complex passwords. Passwords are assigned a maximum age, a minimum length of characters.</p> <p>Password handling requirements include the changing of Contractor supplied default passwords prior to introducing the associated service or system into any Microsoft Online Services owned or operated environment.</p> <p>“User password management and user registration” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 11.2.1 and 11.2.3. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls SA-03 through SA-04

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>SA-03</p> <p>Security Architecture - Data Security / Integrity</p>	<p>Policies and procedures shall be established and mechanisms implemented to ensure security (e.g., encryption, access controls, and leakage prevention) and integrity of data exchanged between one or more system interfaces, jurisdictions, or with a third party shared services provider to prevent improper disclosure, alteration or destruction complying with legislative, regulatory, and contractual requirements.</p>	<p>To minimize the risks associated with the exchange of assets between organizations, exchanges between internal or external organizations are completed in a predefined manner and access to the Microsoft Online Services production environments by staff and Contractor staff is tightly controlled.</p> <p>“Information exchange policies and procedures and information leakage” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 10.8.1 and 12.5.4. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>SA-04</p> <p>Security Architecture - Application Security</p>	<p>Applications shall be designed in accordance with industry accepted security standards (i.e., OWASP for web applications) and complies with applicable regulatory and business requirements.</p>	<p>Security Development Lifecycle: Microsoft applies Security Development Lifecycle, a software security assurance process, to design, develop, and implement Office 365 services. Security Development Lifecycle helps to ensure that communication and collaboration services are highly secured—even at the foundation level. Through controls like Establish Design Requirements, Analyze Attack Surface, and Threat Modeling, Security Development Lifecycle helps Microsoft identify: Potential threats while running a service, Exposed aspects of the service that are open to attack.</p> <p>If potential threats are identified at Design, Development, or Implementation phases, Microsoft can minimize the probability of attacks by restricting services or eliminating unnecessary functions. After eliminating the unnecessary functions, Microsoft reduces these potential threats in the Verification phase by fully testing the controls in the Design phase. More information can be found in: http://www.microsoft.com/security/sdl/</p> <p>Furthermore, we validate the service using third party penetration testing based upon the OWASP top ten.</p> <p>“Control of technical vulnerabilities” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 12.6.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls SA-05 through SA-06

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>SA-05</p> <p>Security Architecture - Data Integrity</p>	<p>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 or corruption of data.</p>	<p>Microsoft Online Services defines acceptable standards to ensure that data inputs to application systems are accurate and within the expected range of values. Where appropriate, data inputs should be sanitized or otherwise rendered safe before being inputted to an application system.</p> <p>Internal processing controls are implemented within the Microsoft Online Services 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, load balancing controls, and job scheduling software.</p> <p>“Correct processing in applications” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 12.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>SA-06</p> <p>Security Architecture - Production / Non-Production Environments</p>	<p>Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets.</p>	<p>Separate environments are maintained for the Non-production and for Production operations of Microsoft Online Services. Access to the production environment is carefully controlled to allow access to Microsoft Online Services and Microsoft Online Services Contractor members who require access and are authorized to perform certain duties.</p> <p>While each environment may have its own standards for operating, a formalized procedure exists for the exchange of Assets between environments. These procedures adhere to all relevant privacy requirements and Services Standards.</p> <p>“Separation of development, test and operational facilities” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.1.4. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls SA-07 through SA-08

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>SA-07</p> <p>Security Architecture - Remote User Multi-Factor Authentication</p>	<p>Multi-factor authentication is required for all remote user access.</p> <p>What forms of authentication are used for operations requiring high assurance? This may include login to management interfaces, key creation, access to multiple-user accounts, firewall configuration, remote access, etc.</p> <p>· Is two-factor authentication used to manage critical components within the infrastructure, such as firewalls, etc.?</p>	<p>Access to the Microsoft Online Services production environments by staff and contractors is tightly controlled.</p> <ul style="list-style-type: none"> • Terminal Services servers are configured to use the high encryption setting. • Microsoft Users have a Microsoft Online Services issued smartcard with a valid certificate and a valid domain account to establish a remote access session. <p>“Microsoft User authentication for external connections” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.4.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>SA-08</p> <p>Security Architecture - Network Security</p>	<p>Network environments shall be designed and configured to restrict connections between trusted and untrusted networks and reviewed at planned intervals, documenting the business justification for use of all services, protocols, and ports allowed, including rationale or compensating controls implemented for those protocols considered to be insecure. Network architecture diagrams must clearly identify high-risk environments and data flows that may have regulatory compliance impacts.</p>	<p>The networks within the Office 365 data centers are designed to create multiple separate network segments. This segmentation helps to provide physical separation of critical, back-end servers and storage devices from the public-facing interfaces.</p> <p>“Segregation in networks” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.4.5. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Control SA-09

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>SA-09</p> <p>Security Architecture - Segmentation</p>	<p>System and network environments are separated by firewalls to ensure the following requirements are adhered to:</p> <ul style="list-style-type: none"> • Business and customer requirements • Security requirements • Compliance with legislative, regulatory, and contractual requirements • Separation of production and non-production environments • Preserve protection and isolation of sensitive data 	<p>The networks within the Office 365 data centers are designed to create multiple separate network segments. This segmentation helps to provide physical separation of critical, back-end servers and storage devices from the public-facing interfaces. Customer access to services provided over the Internet originates from users' Internet-enabled locations and ends at a Microsoft data center. These connections established between customers and Microsoft data centers are encrypted using industry-standard Transport Layer Security (TLS) /Secure Sockets Layer (SSL). The use of TLS/SSL effectively establishes a highly secure browser-to-server connection to help provide data confidentiality and integrity between the desktop and the data center. Filtering routers at the edge of the Office 365 services network provides security at the packet level for preventing unauthorized connections to Office 365 Services.</p> <p>Data storage and processing is logically segregated among customers of the same service through Active Directory® structure and capabilities specifically developed to help build, manage, and secure multitenant environments.</p> <p>The multitenant security architecture ensures that customer data stored in shared Office 365 data centers is not accessible by or compromised to any other organization. Organizational Units (OUs) in Active Directory control and prevent the unauthorized and unintended information transfer via shared system resources. Tenants are isolated from one another based on security boundaries, or silos, enforced logically through Active Directory.</p> <p>“Security of network services” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.6.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls SA-10 through SA-11

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>SA-10</p> <p>Security Architecture - Wireless Security</p>	<p>Policies and procedures shall be established and mechanisms implemented to protect wireless network environments, including the following:</p> <ul style="list-style-type: none"> • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing Contractor default settings (e.g., encryption keys, passwords, SNMP community strings, etc.). • Logical and physical 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 	<p>Protection of wireless devices are part of regular network management security practices which include monitoring. Wireless devices are encrypted and access to the wireless network is managed through multi-factor authentication (smartcard, laptop with trusted module platform chip with Direct Access).</p> <p>Access from a wireless network to the Office 365 environment on customer premise must be secured by the customer.</p> <p>“Network security management” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.6. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>SA-11</p> <p>Security Architecture - Shared Networks</p>	<p>Access to systems with shared network infrastructure shall be restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations.</p>	<p>Microsoft Online Services has procedures as well as automated and semi-automated systems for granting and revoking access to the servers in the "Managed" domain which contain user's apps and data as well as servers in the "Management" domain which provides systems management functions (e.g., monitoring, backup, troubleshooting, software and patch mgmt.). The people in the Microsoft Online "Access and Identity" group manage access via Microsoft Active Directory to the "Managed" and "Management" domains. Authority is granted under the "Least Privilege Access" principle by the Service Managers in each area. Microsoft Online Services users of production systems are restricted to only one User ID per system.</p> <p>Microsoft Online Services ensures that access control and credential management systems are designed and operated to comply with Microsoft Online Services policies and standards. Microsoft Online Services key controls related to Identity and Access management are formally audited annually through the SAS 70 Type II audit for BPOS-D and GFS. In addition, these controls are internally assessed for compliance with Microsoft Online Services policies and standards.</p> <p>“Network security management and user access management” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 10.6 and 11.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>

Office 365 Security Response in the Context of CSA Cloud Control Matrix Controls SA-12 through SA-15

Control ID In CCM	Description (CCM Version R1.1. Final)	Microsoft Response
<p>SA-12</p> <p>Security Architecture - Clock Synchronization</p>	<p>An external accurate, externally agreed upon, time source shall be used to synchronize the system clocks of all relevant information processing systems within the organization or explicitly defined security domain to facilitate tracing and reconstitution of activity timelines. Note: specific legal jurisdictions and orbital storage and relay platforms (US GPS & EU Galileo Satellite Network) may mandate a reference clock that differs in synchronization with the organizations domicile time reference, in this event the jurisdiction or platform is treated as an explicitly defined security domain.</p>	<p>In order to both increase the security of Microsoft Online Services, and to provide accurate reporting detail in event logging and monitoring processes and records, all Microsoft Online Services use consistent clock setting standards (e.g. PST, GMT, UTC etc.). When possible, Microsoft Online Services uses synchronization protocols in order to maintain accurate time throughout the Microsoft Online Services environments.</p> <p>“Clock synchronization” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.10.6. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>SA-13</p> <p>Security Architecture - Equipment Identification</p>	<p>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.</p>	<p>“Equipment identification in networks” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 11.4.3. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>SA-14</p> <p>Security Architecture - Audit Logging / Intrusion Detection</p>	<p>Audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events shall be retained, complying with applicable policies and regulations. Audit logs shall be reviewed at least daily and file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents. Physical and logical user access to audit logs shall be restricted to authorized personnel.</p>	<p>Access to logs is restricted and defined by policy and logs are reviewed on a regular basis.</p> <p>“Audit logging” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.10.1. For more information review of the publicly available ISO standards we are certified against is suggested.</p>
<p>SA-15</p> <p>Security Architecture - Mobile Code</p>	<p>Mobile code shall be authorized before its installation and use, and the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy. All unauthorized mobile code shall be prevented from executing.</p>	<p>Microsoft Online Services is an isolated server centric environment which mobile code isn't as applicable as in a desktop environment. In addition, all code is explicitly installed on our servers by Administrators through the change control process.</p> <p>“Controls against mobile code” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.4.2. For more information review of the publicly available ISO standards we are certified against is suggested.</p>