Microsoft Office 365 Compliance Offerings

March 2021

Microsoft maintains the largest compliance portfolio in the industry both in terms of breadth (total number of offerings), as well as depth (number of customer-facing services in assessment scope). Compliance offerings are grouped into four segments: ***globally applicable****,* ***U.S. government****,* ***industry specific****, and* ***region/country specific****. Each offering description provides an up to-date-scope statement and links to useful downloadable resources.*

This document provides an overview of Office 365 compliance offerings intended to help customers meet their own compliance obligations across regulated industries and markets worldwide.

Contents

Overview

Office 365 is a multi-tenant hyperscale cloud platform and an integrated experience of apps and services, that is available or announced to customers in several regions worldwide. Most Office 365 services enable customers to specify the region where their Customer Data will be located. Microsoft may replicate Customer Data to other regions within the same geo for data resiliency, but Microsoft will not replicate Customer Data outside the chosen geo (e.g. the United States). This document covers the following Office 365 cloud environments:

- **Office 365**, the public cloud service available globally.
- **GCC** (**Government Community Cloud)** which is available for United States Federal, State, Local, and Tribal governments, as well as contractors holding or processing data on behalf of the US Government.
- **GCC High**, which is designed according to Department of Defense (DoD) Security Requirements Guidelines Level 4 controls and supports strictly regulated federal and defense information. This environment is used by federal agencies, the Defense Industrial Base (DIBs), and government contractors.
- **DoD**, which is designed according to DoD Security Requirements Guidelines Level 5 controls and supports strict federal and defense regulations. This environment is for the exclusive use by the US Department of Defense.
- For Office 365 Advanced Threat Protection *Anti-Phishing for user and domain impersonation and spoof intelligence are not yet available in GCC-High and DoD (ETA: TBD)

To help customers meet their own compliance obligations across regulated industries and markets worldwide, Microsoft maintains the largest compliance portfolio in the industry both in terms of breadth (total number of offerings), as well as depth (number of customer-facing services in assessment scope). To find out which services are available in which regions, customers can explore International availability and the Where is your data located? site. To find out more information about Office 365 Government cloud environment customers can explore the Office 365 Government Cloud site.

Compliance offerings are grouped into four segments: **globally applicable, US government, industry specific, and region/country specific**. Compliance offerings are based on various types of assurances, including formal certifications, attestations, validations, authorizations, and assessments produced by independent third-party auditing firms, as well as contractual amendments, self-assessments, and customer guidance documents produced by Microsoft. Each offering description in this document provides an up to date scope statement indicating which customer-facing services are in scope for the assessment, as well as links to downloadable resources to assist customers with their own compliance obligations. Several compliance offerings are also available as self-service risk assessments in Compliance Manager, as noted throughout the document.

More detailed information about Microsoft's compliance offerings is available from the Trust Center. Moreover, all downloadable documentation is available to customers under a non-disclosure agreement from the Service Trust Portal in sections labeled:

- Audit Reports, which is further divided into ISO, SOC, and other sections; and
- Data Protection Resources, which is further divided into Compliance Guides, FAQ and Whitepapers, Pen Test and Security Assessments, and other sections.

Customers are wholly responsible for ensuring their own compliance with all applicable laws and regulations. Information provided in this document does not constitute legal advice, and customers should consult their legal advisors for any questions regarding regulatory compliance.

Globally Applicable

Compliance offerings covered in this section have global applicability across regulated industries and markets. They can often be relied upon by customers when addressing specific industry and regional compliance obligations. For example, ISO 27001 certification provides a baseline set of requirements for many other international standards and regulations.

1 CSA Cloud Control Matrix

The Cloud Security Alliance (CSA) is a nonprofit organization led by a broad coalition of industry practitioners, corporations, and other important stakeholders. It is dedicated to defining best practices to help ensure a more secure cloud computing environment, and to helping potential cloud customers make informed decisions when transitioning their IT operations to the cloud. In 2013, the CSA and the British Standards Institution launched the Security, Trust & Assurance Registry (STAR), a free, publicly accessible registry in which cloud service providers (CSPs) can publish their CSA-related assessments based on the Cloud Controls Matrix (CCM), a controls framework covering fundamental security principles across 16 domains to help cloud customers assess the overall security risk of a CSP. For the CSA STAR Self-Assessment, Microsoft publishes CCM-based reports for Office 365, and a CSA CCM Assessment for Office 365 is available in Compliance Manager.

Applicability	Services in scope
Office 365	Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Office Online, Office Services Infrastructure, Office 365 Customer Portal

2 ISO 27001:2013

The ISO 27000 family of standards provide a framework for policies and procedures that include all legal, physical, and technical controls involved in an organization's information risk management processes. ISO 27001 specifies the requirements for implementing, maintaining, monitoring, and continually improving an information security management standard (ISMS).[1] The 2013 update added a section on outsourcing which reflects the facts that many organizations rely on cloud service providers to provide some aspects of IT. Office 365 maintains its ISO 27001 certification and makes the corresponding audit report and certificate available to customers from the Service Trust Portal, and an ISO 27001 Assessment for Office 365 is available in Compliance Manager.

[1] ISO 27002 provides guidelines and best practices for information security management; however, an organization cannot get certified against ISO 27002 because it is not a management standard. The audit vehicle is ISO 27001, which relies on detailed guidelines in ISO 27002 for control implementation.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Azure Communications Service, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection, Access Online, Project Online, Office Services Infrastructure, Office 365 Customer Portal, Identity Manager, Service Encryption with Customer Key, Lockbox (Torus), Customer Lockbox, Griffin, Office 365 Microservices (including but not limited to Kaizala, ObjectStore, Sway, PowerPoint Online Document Service, Query Annotation Service, School Data Sync, Siphon, Speech, StaffHub, eXtensible Application Program)
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Azure Communications Service, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection
GCC High	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Azure Communications Service, Planner, Forms, PowerApps, Flow, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection
DoD	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Azure Communications Service, Planner, Forms, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection

3 ISO 27017:2015

The ISO 27017 code of practice is designed for organizations to use as a reference for selecting cloud services information security controls when implementing a cloud computing information security management system based on ISO 27002. It can also be used by cloud service providers as a guidance document for implementing commonly accepted protection controls. This international standard provides additional cloud-specific implementation guidance based on ISO/IEC 27002, and provides additional controls to address cloud-specific information security threats and risks. The Office 365 ISO 27017 audit report is available for download. ISO 27017 is unique in providing guidance for both cloud service providers and cloud service customers. It also provides cloud service customers with practical information on what they should expect from cloud service providers. Customers can benefit directly from ISO 27017 by ensuring they understand the concept of shared responsibilities in the cloud.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Azure Communications Service, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection, Access Online, Project Online, Office Services Infrastructure,

Applicability	Services in scope
	Office 365 Customer Portal, Identity Manager, Service Encryption with Customer Key, Lockbox (Torus), Customer Lockbox, Griffin, Office 365 Microservices (including but not limited to Kaizala, ObjectStore, Sway, PowerPoint Online Document Service, Query Annotation Service, School Data Sync, Siphon, Speech, StaffHub, eXtensible Application Program)
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Azure Communications Service, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection
GCC High	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Azure Communications Service, Planner, Forms, PowerApps, Flow, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection
DoD	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Azure Communications Service, Planner, Forms, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection

4 ISO 27018:2019

ISO 27018 is the first international code of practice for cloud privacy that provides guidelines based on ISO 27002 guidelines and best practices for information security management. Based on EU data-protection laws, it gives specific guidance to cloud service providers acting as processors of personally identifiable information (PII) on assessing risks and implementing state-of-the-art controls for protecting PII. ISO 27018 establishes cloud-specific control objectives and guidelines for PII in accordance with the privacy principles in ISO 29100. The Office 365 ISO 27018 audit report is available for download from the Service Trust Portal, and an ISO 27018 Assessment for Office 365 is available in Compliance Manager.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Azure Communications Service, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection, Access Online, Project Online, Office Services Infrastructure, Office 365 Customer Portal, Identity Manager, Service Encryption with Customer Key, Lockbox (Torus), Customer Lockbox, Griffin, Office 365 Microservices (including but not limited to Kaizala, ObjectStore, Sway, PowerPoint Online Document Service, Query Annotation Service, School Data Sync, Siphon, Speech, StaffHub, eXtensible Application Program)
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Azure Communications Service, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection

GCC High	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Azure Communications Service, Planner, Forms, PowerApps, Flow, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection
DoD	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Azure Communications Service, Planner, Forms, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection

5 SOC 1

The American Institute of Certified Public Accountants (AICPA) has established three Service Organization Controls (SOC) reporting options (SOC 1, SOC 2, and SOC 3) to assist CPAs with examining and reporting on a service organization's controls. The SOC 1 attestation is based on the AICPA Statement on Standards for Attestation Engagements 16 (SSAE 16) standard (see AT-C Section 105) and the International Standard on Assurance Engagements No. 3402 (ISAE 3402). A SOC 1 report includes auditor's opinion on the control effectiveness to achieve the related control objectives during the specified monitoring period. Customers can leverage the Office 365 SOC 1 attestation when pursuing their own financial industry specific compliance requirements such as Sarbanes-Oxley (SOX), Federal Financial Institutions Examination Council (FFIEC), Gramm-Leach-Bliley Act (GLBA), etc. Office 365 maintains a SOC 1 attestation that is based on a rolling 12-month run window (audit period) with new reports issued annually. Customers can download the latest attestation report from the Service Trust Portal.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Teams, Planner, Forms, PowerApps, MyAnalytics, PowerBI, Compliance Manager, Project Online, Office Services Infrastructure, Office 365 Customer Portal, Identity Manager, Service Encryption with Customer Key, Lockbox (Torus), Customer Lockbox, Griffin, Office 365 Microservices (including but not limited to Kaizala, ObjectStore, Sway, PowerPoint Online Document Service, Query Annotation Service, School Data Sync, Siphon, Speech, StaffHub, eXtensible Application Program)
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection
GCC High	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection
DoD	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Planner, Forms, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection

6 SOC 2

SOC 2 is a restricted use report intended to report on controls relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy system attributes. SOC 2 engagements are conducted in accordance with the Trust Services Principles and Criteria, as well as the requirements stated in the AICPA SSAE 18 standard. In addition, the Office 365 SOC 2 report addresses the requirements set forth in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM). Office 365 SOC 1 and SOC 2 attestations are based on rigorous independent third-party audits conducted by a reputable CPA firm. At the end of a SOC 1 or SOC 2 audit, the auditor renders an opinion in a SOC 1 or SOC 2 report, which describes the cloud service provider's (CSP's) system and assesses the fairness of the CSP's description of its controls. It also evaluates whether the CSP's controls are designed appropriately, were in operation on a specified date, and were operating effectively over a specified time period. The Office 365 SOC 2 report is relevant to the Security, Availability, Confidentiality, and Processing Integrity trust principles. Office 365 maintains a SOC 2 attestation that is based on a rolling 12-month run window (audit period) with new reports issued annually. Customers can download the latest attestation report, along with Office 365 Additional Services reports and Bridge Letters from the Service Trust Portal.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Teams, Planner, Forms, PowerApps, MyAnalytics, PowerBI, Compliance Manager, Project Online, Office Services Infrastructure, Office 365 Customer Portal, Identity Manager, Service Encryption with Customer Key, Lockbox (Torus), Customer Lockbox, Griffin, Office 365 Microservices (including but not limited to Kaizala, ObjectStore, Sway, PowerPoint Online Document Service, Query Annotation Service, School Data Sync, Siphon, Speech, StaffHub, eXtensible Application Program)
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection
GCC High	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection
DoD	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Planner, Forms, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection

7 SOC 3

A SOC 3 report is a short, publicly facing version of the SOC 2 attestation report, for users who want assurances about the cloud service provider's controls but do not need a full SOC 2 report. Azure SOC 3 report can be downloaded from the Service Trust Portal.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Teams, Planner, Forms, PowerApps, MyAnalytics, PowerBI, Compliance Manager, Project Online, Office Services Infrastructure, Office 365 Customer Portal, Identity Manager, Service Encryption with Customer Key, Lockbox (Torus), Customer Lockbox, Griffin, Office 365 Microservices (including but not limited to Kaizala, ObjectStore, Sway, PowerPoint Online Document Service, Query Annotation Service, School Data Sync, Siphon, Speech, StaffHub, eXtensible Application Program)
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection
GCC High	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection
DoD	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Planner, Forms, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection

8 WCAG 2.0 (ISO 40500:2012)

The Web Content Accessibility Guidelines 2.0 (WCAG 2.0) provide a framework for developing web content that improves accessibility for people with disabilities, as well as users of devices with limited graphical abilities. WCAG 2.0 was published in 2008 by the World Wide Web Consortium (W3C). In 2012, WCAG 2.0 was also published by the International Organization for Standardization (ISO) as ISO/IEC 40500:2012.

WCAG 2.0 is organized around four principles, which in turn have 12 guidelines. Each guideline has testable success criteria, which are scored at three conformance levels: A, AA, and AAA. Microsoft publishes WCAG 2.0 AA reports that reflect the complete product or service. We generally do not create a report for individual features or components. In some cases, we may release a new component for an existing product, or a new version of an existing component, which users may choose to install separately, and we may publish a WCAG 2.0 AA report for that component.

Applicability	Services in Scope
Office 365	Excel, Exchange Admin Center, Office 365 Admin Center (Portal), Office 365 and Azure AD login experience, Office 365 Security & Compliance Center, Office 365 Video, Office Lens, Office.com, OneDrive Admin Center, OneDrive for Business, OneDrive Sync Client, OneNote, Orcas, Outlook, Outlook Groups, PowerPoint, Project, Office 365 Customer Portal, Word See list of WCAG 2.0 AA reports for full list of Microsoft products and versions.

GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection
GCC High	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection
DoD	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Planner, Forms, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection

US Government

The following compliance offerings are focused primarily on addressing the needs of the United States Government. Office 365, Office 365 Government, and Office 365 Government Defense have the same comprehensive security controls in place, as well as the same Microsoft commitment on the safeguarding of Customer Data. Office 365 Government provides additional controls regarding U.S. Government-specific background screening requirements, including maintaining U.S. persons for Office 365 Government operations. Office 365 Government Defense is reserved for exclusive use by the United States Department of Defense.

9 CJIS

The Criminal Justice Information Services (CJIS) Division of the US Federal Bureau of Investigation (FBI) gives state, local, and federal law enforcement and criminal justice agencies access to criminal justice information (CJI)—for example, fingerprint records and criminal histories. Law enforcement and other government agencies in the United States must ensure that their use of cloud services for the transmission, storage, or processing of CJI complies with the CJIS Security Policy, which establishes minimum security requirements and controls to safeguard CJI. All private contractors who process CJI must sign the CJIS Security Addendum, a uniform agreement approved by the US Attorney General that helps ensure the security and confidentiality of CJI required by the Security Policy. It also commits the contractor to maintaining a security program consistent with federal and state laws, regulations, and standards, and limits the use of CJI to the purposes for which a government agency provided it.

Microsoft will sign the CJIS Security Addendum in states with CJIS Information Agreements. These agreements tell state law enforcement authorities responsible for compliance with CJIS Security Policy how Microsoft's cloud security controls help protect the full lifecycle of data and ensure appropriate background screening of operations personnel with potential access to CJI. Microsoft continues to work with state governments to enter into CJIS Information Agreements. Microsoft has agreements signed with 34 states, including Alabama, Alaska, Arkansas, Arizona, California, Colorado, Florida, Georgia, Hawaii, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Massachusetts, Michigan, Minnesota, Missouri, Montana, New Jersey, New York, Nevada, North Carolina, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Washington.

Customers subject to CJIS requirements should review the CJIS Implementation Guidelines for Office 365 U.S. Government. Also available is the Microsoft Cloud – CJIS Cloud Computing Requirements Mapping, which details CJIS specific requirements and Microsoft cloud provider's responses.

Applicability	Services in scope
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection

10 DFARS

Defense contractors whose information systems process, store, or transmit covered defense information (CDI) must comply with the Department of Defense (DoD) Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, which specifies requirements for the protection of controlled unclassified information (CUI) in accordance with NIST SP 800-171, cyber incident reporting obligations, and other considerations for cloud service providers. All DoD contractors are required to comply with DFARS requirements for adequate security "as soon as practical, but not later than 31 December 2017.

Office 365 Government has attained a FedRAMP Moderate Provisional Authorization to Operate (P-ATO) as well as a DoD DISA SRG Level 4 Provisional Authorization (PA) whereas Office 365 Government Defense has attained a DoD DISA SRG Level 5 PA. These authorizations allow DoD mission partners to host CDI within the Office 365 Government and Office 365 Government Defense clouds. Microsoft provides a contract amendment to help defense contractors meet the requirements in the DFARS Clause 252.204-7012 that apply to cloud service providers. When defense contractors are required to include the DFARS Clause 252.204-7012 flow-downs in subcontracts, Microsoft can accept the flow-down terms applicable to cloud service providers for Office 365 Government and Office 365 Government Defense. See Microsoft Cloud Service Authorizations. GCC environment does not have flow downs.

Applicability	Services in scope
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection
GCC High	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection
DoD	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Planner, Forms, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection

11 DoD DISA SRG Level 2

The Defense Information Systems Agency (DISA) is an agency of the US Department of Defense (DoD) that is responsible for developing and maintaining the DoD Cloud Computing Security Requirements Guide (SRG). The SRG defines the baseline security requirements used by DoD to assess the security posture of a cloud service provider (CSP), supporting the decision to grant a DoD Provisional Authorization (PA) that allows a CSP to host DoD missions. It incorporates, supersedes, and rescinds the previously published DoD Cloud Security Model (CSM).

Office 365 maintains a DoD PA at SRG Impact Level 2 (IL2), which covers non-controlled unclassified information including all data cleared for public release, for the in-scope services.

Applicability	Services in scope
GCC	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Delve, People Card, Teams, Office Service Infrastructure, Intelligent Services, Office 365 Customer Portal, Bing Services, Windows Ink, Activity Feed Service, Usage Reports

12 DoD DISA SRG Level 4

While Office 365 does not currently hold a DoD PA at SRG Impact Level 4 (IL4), customers that require an IL4 PA can accredit Office 365 (GCC High) themselves. Office 365 DoD maintains an IL5 PA and can therefore store IL4 data. DoD customers that require storage of IL4 data could use Office 365 DoD for this capability.

13 DoD DISA SRG Level 5

Office 365 Government Defense maintains a DoD Provisional Authorization (PA) at SRG Impact Level 5 (IL5), which accommodates CUI that may require a higher level of protection than that afforded by IL4, for the in-scope services. Moreover, IL5 supports unclassified National Security Systems.

Applicability	Services in scope
DoD	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, People Card, Teams, Office Service Infrastructure, Intelligent Services, Office 365 Customer Portal, Bing Services, Windows Ink, Activity Feed Service, Usage Reports

14 FedRAMP Moderate (NIST SP 800-53)

The US Federal Risk and Authorization Management Program (FedRAMP) was established in December 2011 to provide a standardized approach for assessing, monitoring, and authorizing cloud service providers (CSPs). CSPs desiring to sell services to a federal agency requiring FedRAMP can take three paths to demonstrate FedRAMP compliance: 1) earn a Provisional Authorization to Operate (P-ATO) from the Joint Authorization Board (JAB); 2) receive an Authorization to Operate (ATO) from a federal agency; or 3) work independently to develop a CSP Supplied Package that meets program requirements. Each of these paths requires a stringent technical review by the FedRAMP Program Management Office and an assessment by an independent third-party assessment organization that is accredited by the program.

FedRAMP is based on the National Institute of Standards and Technology (NIST) SP 800-53 Rev 4 standard, augmented by FedRAMP controls and enhancements. FedRAMP authorizations are granted at three impact levels based on the NIST FIPS 199 guidelines—Low, Moderate, and High. These levels rank the impact that the loss of confidentiality, integrity, or availability could have on an organization—Low (limited effect), Moderate (serious adverse effect), and High (severe or catastrophic effect). The number of controls in the corresponding baseline increases as the impact level increases, e.g., FedRAMP Moderate baseline has 325 controls whereas FedRAMP High baseline has 421 controls.

Office 365 (Enterprise, and GCC) was granted a FedRAMP Agency ATO at the Moderate Impact Level by the Department of Health and Human Services Office of the Inspector General. GCCH has a High Agency ATO from the Department of Justice, and DoD has a High/L5 P-ATO from DISA.

Office 365 Assessments for both FedRAMP Moderate and NIST 800-53 are available in Compliance Manager.

Applicability	Services in scope
GCC	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Delve, People Card, Teams, Office Service Infrastructure, Intelligent Services, Office 365 Customer Portal, Bing Services, Windows Ink, Activity Feed Service, Usage Reports
GCC High	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, People Card, Teams, Office Service Infrastructure, Intelligent Services, Office 365 Customer Portal, Bing Services, Windows Ink, Activity Feed Service, Usage Reports
DoD	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, People Card, Teams, Office Service Infrastructure, Intelligent Services, Office 365 Customer Portal, Bing Services, Windows Ink, Activity Feed Service, Usage Reports

15 FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government standard that defines minimum security requirements for cryptographic modules in products and systems. Validation against the FIPS 140-2 standard is required for all US federal government agencies that use cryptography-based security systems to protect sensitive but unclassified information stored digitally. NIST publishes a list of vendors and their cryptographic modules validated for FIPS 140-2. Microsoft certifies the cryptographic modules used in Microsoft products with each new release of the Windows operating system, and Office 365 relies on FIPS 140-2 validated modules in the underlying operating system. Moreover, customers can store their own cryptographic keys and other secrets in FIPS 140-2 validated hardware security modules (HSM).

Applicability	Validated cryptographic modules
Office 365 GCC GCC High DoD	See Microsoft's current validations.

16 IRS 1075

Internal Revenue Service Publication 1075 (IRS 1075) provides safeguards for protecting Federal Tax Information (FTI) at all points where it is received, processed, stored, and maintained. It applies to federal, state, and local agencies with whom IRS shares FTI, and it defines a broad set of management, operations, and technology specific security controls that must be in place to protect FTI. The core control scope is based on NIST SP 800-53 R4 that Office 365 U.S. Government covers as part of the existing FedRAMP authorization. Additional requirements cover protection of FTI in a cloud computing environment, and place much emphasis on FIPS 140-2 validated data encryption in transit and at rest.

Microsoft can provide customers with contractual commitment to demonstrate that Office 365 U.S. Government has appropriate security controls and capabilities in place necessary for customers to meet the substantive IRS 1075 requirements. Customers can download the Office 365 IRS 1075 Safeguard Security Report from the Service Trust Portal to understand how Office 365 U.S. Government implements the applicable IRS controls. Moreover, Microsoft provides another document, Office 365 MT Government Compliance Considerations, directly to the IRS to outline how an agency can use Office 365 U.S. Government services in a way that complies with IRS 1075 requirements.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Delve, People Card, Teams, Office Service Infrastructure, Intelligent Services, Office 365 Customer Portal, Bing Services, Windows Ink, Activity Feed Service, Usage Reports
GCC	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Delve, People Card, Teams, Office Service Infrastructure, Intelligent Services, Office 365 Customer Portal, Bing Services, Windows Ink, Activity Feed Service, Usage Reports

17 ITAR

The US Department of State has export control authority over defense articles, services, and related technologies under the International Traffic in Arms Regulations (ITAR) managed by the Directorate of Defense Trade Controls (DDTC). Items under ITAR protection are documented on the US Munitions List (USML). While there is no ITAR compliance certification, Microsoft has implemented controls in Office 365 U.S. Government Defense to support customers subject to ITAR obligations. Microsoft also offers additional support to customers with data subject to ITAR through contractual commitments regarding the location of stored data, as well as limitations on Microsoft's potential access to such data to US persons.

Customers who are manufacturers, exporters, and brokers of defense articles, services, and related technologies as defined on the USML must be registered with DDTC, must understand and abide by ITAR, and must self-certify that they operate in accordance with ITAR. Customers with ITAR-controlled data are eligible for enrollment in Office 365 U.S. Government Defense provided they sign additional agreements formally notifying Microsoft of their intention to store ITAR-controlled data so that Microsoft may comply with responsibilities both to customers and to the US government.

Applicability	Services in scope

GCC High	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, People Card, Teams, Office Service Infrastructure, Intelligent Services, Office 365 Customer Portal, Bing Services, Windows Ink, Activity Feed Service, Usage Reports
DoD	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, People Card, Teams, Office Service Infrastructure, Intelligent Services, Office 365 Customer Portal, Bing Services, Windows Ink, Activity Feed Service, Usage Reports

18 NIST Cybersecurity Framework

The NIST Cybersecurity Framework (NIST CSF) is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risk. Created through collaboration between industry and United States Government, the framework is designed to promote the protection of critical infrastructure. Version 1.0 of the Framework was prepared by NIST, with extensive private sector input and issued in February 2014. The most recent version, Framework V1.1 was released on April 16, 2018 following a 45-day public comment period on the second draft of Framework V1.1.

Based on the results of a HITRUST CSF-validated assessment performed by an approved HITRUST CSF Assessor organization and documented in a HITRUST CSF Assessment Report, the services in scope below have been certified by the HITRUST Alliance as being supported by an information protection program that is consistent with the objectives specified in NIST CSF. HITRUST's NIST Letter of Certification for these services is available for download from the Service Trust Portal. A NIST CSF Assessment for Office is also available in Compliance Manager.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, People Card, Teams, Office Service Infrastructure, Intelligent Services, Office 365 Customer Portal, Bing Services, Windows Ink, Activity Feed Service, Usage Reports

19 NIST SP 800-171

NIST SP 800-171 provides guidelines for the protection of CUI in nonfederal information systems and organizations. Mapping tables in Appendix D (D1 through D14) provide control mapping between CUI security requirements and relevant security controls in NIST SP 800-53, indicating that NIST SP 800-171 represents a subset of the NIST SP 800-53 controls for which Office 365 has already been assessed and authorized under the FedRAMP program. Consequently, customers can be assured that FedRAMP Moderate baseline addresses fully and exceeds the requirements of NIST SP 800-171. Therefore, all Office 365 U.S. Government and Office 365 U.S. Government Defense services that have received FedRAMP authorizations conform to the NIST SP 800-171 requirements and can accommodate customers looking to deploy CUI workloads. A NIST 800-171 Assessment for Office 365 is available in Compliance Manager.

Applicability	Services in scope
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, People Card, Teams, Office Service Infrastructure, Intelligent

Applicability	Services in scope
	Services, Office 365 Customer Portal, Bing Services, Windows Ink, Activity Feed Service, Usage Reports
GCC High	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, People Card, Teams, Office Service Infrastructure, Intelligent Services, Office 365 Customer Portal, Bing Services, Windows Ink, Activity Feed Service, Usage Reports
DoD	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, People Card, Teams, Office Service Infrastructure, Intelligent Services, Office 365 Customer Portal, Bing Services, Windows Ink, Activity Feed Service, Usage Reports

20 FERPA

The Family Educational Rights and Privacy Act (FERPA) is a US federal law that protects the privacy of students' education records, including personally identifiable and directory information. FERPA was enacted to ensure that parents and students age 18 and older can access those records, request changes to them, and control the disclosure of information, except in specific and limited cases where FERPA allows for disclosure without consent. The law applies to schools, school districts, and any other institution that receives funding from the US Department of Education—that is, virtually all public K–12 schools and school districts, as well as most post-secondary institutions, both public and private.

FERPA does not require or recognize audits or other certifications, so any academic institution that is subject to FERPA must assess for itself whether and how its use of a cloud service affects its ability to comply with FERPA requirements. In its Online Services Terms, Microsoft agrees to be designated as a "school official" with "legitimate educational interests" in Customer Data as defined under FERPA. Customer Data would include any student records provided to Microsoft through a school's use of Office 365. When handling student education records in Customer Data, Microsoft agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) just as school officials do.

COPPA and CIPA are additional laws intended to protect the privacy of children; however, they are not directly applicable to Office 365. The Children's Online Privacy Protection Act (COPPA) is a US federal law enacted to protect the privacy of children under 13. Its enforcement is managed by the Federal Trade Commission (FTC). COPPA applies to websites and online services directed to children and stipulates that these sites and services must require parental consent for the collection and use of any personal information belonging to children. The Children's Internet Protection Act (CIPA) was enacted to address concerns about children's access to harmful content over the Internet. The Federal Communications Commission (FCC) issued rules implementing CIPA and defined requirements for schools and libraries subject to CIPA. Customers enquiring about COPPA and CIPA in the context of Office 365 adoption should review the section titled Educational Institutions in the Online Services Terms where we explain that customers are responsible for obtaining any parental consent for any end user's use of Microsoft online services.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance

Applicability	Services in scope
	Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection, Azure Information Protection, Bookings, Flow, Kaizala, Microsoft Analytics, Microsoft Booking, Microsoft Graph, Microsoft StaffHub, Microsoft To-Do for Web, Office 365 Cloud App Security, Office 365 Groups, Office 365 Video, Sway, Yammer Enterprise
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection,
GCC High	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection
DoD	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Planner, Forms, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection

21 Section 508 VPATs

Section 508 is an amendment to the Rehabilitation Act of 1973, a US federal law. Section 508 requires US federal government agencies to give employees and members of the public with disabilities access to electronic information and technology that is comparable to access available to others. Agencies must also consider accessibility when purchasing or using information technology.

A Voluntary Product Accessibility Template (VPAT) is a standardized form developed by the Information Technology Industry Council to document whether a product meets key Section 508 requirements. Federal procurement officers and other buyers can use completed templates to help evaluate products they are considering. Microsoft offers detailed VPATs for many Office 365 services, describing the accessibility features of those services. See Section 508 VPATs for other Microsoft products.

Applicability	VPATs
Office 365	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection, Office 365 Business Center, Office 365 Web Suite, Office 365 admin portal for Android, Office 365 admin portal for iOS, Office 365 admin portal, Office 365 and Azure AD sign-in, Office 365 Video, Office Configuration Tool, Office Lens, OneDrive, OneNote, Outlook, Outlook Groups, Access, Excel, Kaizala, Bookings, StaffHub, Word, SharePoint, Visio, To-Do, Yammer
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI,

Applicability	VPATs
	Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection
GCC High	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection
DoD	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Azure Active Directory, Teams, Planner, Forms, Office Pro Plus, Security and Compliance Center, PowerBI, Advanced Compliance, Office 365 Advanced Threat Protection

Industry Specific

The following compliance offerings are intended to address the needs of customers subject to various industry regulations such as those in financial services, healthcare and life sciences, media and entertainment, education, etc. Office 365 is not subject directly to oversight by these regulators; however, Office 365 can help customers meet their own compliance requirements by furnishing a variety of documents ranging from formal independent third-party assessments to guidance documentation and contractual commitments produced by Microsoft.

22 23 NYCRR 500 (USA)

The State of New York recently adopted a rule that imposes a new set of cybersecurity requirements (23 NYCRR 500) on financial institutions that are licensed or authorized to do business by the New York State Department of Financial Services (DFS). This regulation is designed to protect customer data and the information technology systems of regulated institutions. It requires each financial institution to assess its specific risk profile and design a program that addresses the risks. Microsoft has prepared a document (Microsoft Cloud – NYDFS) to explain how Office 365 can help financial institutions comply with 23 NYCRR 500 requirements.

Applicability	Services in scope
Office 365	Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Office Online, Office Services Infrastructure, Office 365 Customer Portal

23 APRA (Australia)

The Australian Prudential Regulation Authority (APRA) oversees banks, credit unions, insurance companies, and other financial services institutions (FSIs) in Australia. Recognizing the momentum towards cloud computing, APRA has called on regulated entities to implement a thoughtful cloud adoption strategy with effective governance, thorough risk assessment, and regular assurance processes. APRA's information paper, "Outsourcing involving shared computing services (including cloud)," outlines important guidance for regulated entities in their assessment of cloud providers and

cloud services. Moreover, when outsourcing a "material business activity[2]," regulated institutions must comply with APRA's outsourcing guidelines, "Prudential Standard CPS 231 Outsourcing."

Customers should review the Microsoft Response to the APRA Information Paper on Cloud, which follows the structure and topics of the APRA document on outsourcing. Microsoft's paper provides a detailed response to each issue raised by APRA to demonstrate how FSIs can move to Office 365 and comply with the APRA guidance. The Microsoft APRA Compliance Checklist for Australian FSIs also covers the regulatory issues that need to be addressed under regulations such as APRA CPS 231, and maps Office 365 against each of those requirements. More information is available on the Australian FSI Trusted Cloud site.

Applicability	Services in scope
Office 365	Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Office Online, Office Services Infrastructure, Office 365 Customer Portal

24 FFIEC (USA)

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body comprised of five banking regulators that is responsible for the federal examination of financial institutions in the United States. The FFIEC Examiner Education Office publishes IT Examination Handbooks intended for field examiners from the FFIEC member agencies. The FFIEC Audit IT Examination Handbook contains guidance on third-party reviews of technology service providers that enables financial institutions to review sufficiently detailed independent audit reports of technology service providers (TSPs) as part of their overall responsibility to manage their relationships with TSPs. Specifically, AICPA's SOC 1, SOC 2, and SOC 3 attestation reports are mentioned in the Audit Handbook as examples of independent audit reports pertinent to TSPs. However, FFIEC also mentions that financial institutions should not rely solely on the information contained in these reports and should instead use additional verification and monitoring procedures discussed in more detail in the FFIEC Outsourcing Technology Services IT Examination Handbook.

Office 365 provides financial institutions with SOC 1 Type 2 and SOC 2 Type 2 attestation reports produced by an independent CPA firm to help customers meet their own FFIEC compliance obligations. For example, the SOC 1 Type 2 attestation is based on the AICPA SSAE 18 standard (see AT-C Section 105) that replaced SAS 70, and it is appropriate for reporting on controls at a service organization relevant to user entities internal controls over financial reporting. This is the formal audit that financial institutions can leverage for third-party reviews of technology service providers when pursuing their own FFIEC specific compliance obligations for assets deployed to Office 365. It includes the auditor's opinion on control effectiveness to achieve the related control objectives during the specified monitoring period.

An FFIEC Assessment for Office 365 that is based on the Information Technology handbook is available in Compliance Manager. Microsoft has also developed an Excel-based Office 365 Cloud Security Diagnostic Tool for performing risk assessments that financial institutions may want to conduct relative to cloud services. The tool is based on a spreadsheet featuring 19 tabs (each for a separate information security

[2] A "material business activity" is an activity that has the potential, if disrupted, to have a significant impact on the financial institution's business operations or ability to manage its risks effectively.

domain) that track requirements set forth by relevant standards and financial services regulations, including FFIEC IT Examination Handbooks. The tool is prepopulated with explanations how Office 365 complies with requirements applicable to cloud service providers and can assist customers in meeting their own FFIEC compliance requirements.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection, Azure Information Protection, Bookings, Exchange Online Protection, Kaizala, Microsoft Analytics, Microsoft Booking, Microsoft Graph, Microsoft StaffHub, Microsoft To-Do for Web, Office 365 Cloud App Security, Office 365 Groups, Office 365 Video, Sway, Yammer Enterprise
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection

25 FISC (Japan)

The Center for Financial Industry Information Systems (FISC) is a not-for-profit organization established by the Japanese Ministry of Finance in 1984 to promote security in banking information systems. Some 700 corporations in Japan are supporting members, including major financial institutions, insurance and credit companies, securities firms, computer manufacturers, and telecommunications enterprises.

In collaboration with its member institutions, the Bank of Japan, and the Financial Services Agency, the FISC created guidelines for the security of banking information systems. These guidelines include basic auditing standards for computer system controls, contingency planning in the event of a disaster, and development of security policies and standards encompassed in more than 300 controls.

Although the application of these guidelines in a cloud computing environment is not required by regulation, most financial institutions in Japan that implement cloud services have built information systems that satisfy these security standards. FISC Guidelines Version 8 Supplemental Revised, issued in 2015, added two revisions relating to the use of cloud services by financial institutions and countermeasures against cyberattacks. Microsoft engaged outside assessors to validate that Office 365 meets the FISC Version 8 requirements. Customers can download "Microsoft Cloud – Response to New FISC Guidelines in Japan" from the Service Trust Portal.

Applicability	Services in scope
Office 365	Access Online, Azure Active Directory, Exchange Online, Exchange Online Protection, Teams, Office 365 ProPlus, Office Delve, Office Online, OneDrive for Business, Power BI for Office 365, Project Online, SharePoint Online, Skype for Business

26 GLBA (USA)

The Gramm-Leach-Bliley Act (GLBA) is a US federal law that reformed the financial services industry and addressed concerns about consumer privacy protection. It required the Federal Trade Commission (FTC) and other financial services regulators to implement regulation addressing GLBA privacy provisions such as the Financial Privacy Rule and Safeguards Rule. GLBA requirements to safeguard sensitive consumer data apply to financial institutions that offer financial products and services to consumers (e.g., loans, investment advice, etc.). Office 365 can help customers comply with the security requirements of the GLBA by providing technical and organizational safeguards to help customers maintain security and prevent unauthorized usage.

Microsoft has developed an Excel-based cloud risk assessment tool that customers can download from the Data Protection | Compliance Guides area of the Service Trust Portal. This tool is meant to expedite a risk assessment that a financial institution may want to conduct relative to cloud services. The tool is based on a spreadsheet featuring 19 tabs (each for a separate information security domain) that track requirements set forth by relevant standards and financial services regulations, including GLBA (see Column R in the spreadsheet). The tool is prepopulated with explanations how Office 365 complies with requirements applicable to cloud service providers and can assist customers in meeting their own compliance requirements, including the security requirements of GLBA.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection, Azure Information Protection, Bookings, Exchange Online Protection, Kaizala, Microsoft Analytics, Microsoft Booking, Microsoft Graph, Microsoft StaffHub, Microsoft To-Do for Web, Office 365 Cloud App Security, Office 365 Groups, Office 365 Video, Sway, Yammer Enterprise
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection

27 GxP (US FDA 21 CFR Part 11)

Microsoft can help customers meet their requirements under Good Clinical, Laboratory, and Manufacturing Practices (GxP), as well as regulations enforced by the US Food and Drug Administration (FDA) under 21 CFR Part 11. There is no GxP or 21 CFR Part 11 certification for cloud service providers; however, Office 365 has undergone independent third-party audits for quality management and information security, including ISO 27001 among many others. Customers using Office 365 should determine the GxP requirements that apply to the computerized system based on its intended use and follow internal procedures governing qualification and/or validation processes to demonstrate that the GxP requirements are met.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection, Azure Information Protection, Bookings, Exchange Online Protection, Kaizala, Microsoft Analytics, Microsoft Booking, Microsoft Graph, Microsoft StaffHub, Microsoft To-Do for Web, Office 365 Cloud App Security, Office 365 Groups, Office 365 Video, Sway, Yammer Enterprise
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection

28 HIPAA and the HITECH Act (USA)

The Health Insurance Portability and Accountability Act (HIPAA) is a US law that establishes requirements for the use, disclosure, and safeguarding of protected health information (PHI). It applies to covered entities—doctors' offices, hospitals, health insurers, and other healthcare companies—with access to PHI, as well as to business associates, such as cloud service providers, that process PHI on their behalf. The scope of HIPAA was extended with the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act that was created to stimulate the adoption of electronic health records and supporting information technology.

HIPAA regulations require that covered entities and their business associates enter into a contract called a Business Associate Agreement (BAA) to ensure the business associates will protect PHI adequately. Microsoft has enabled the physical, technical, and administrative safeguards required by HIPAA and the HITECH Act inside the in-scope cloud services, and offers a HIPAA BAA as part of the Microsoft Online Services Terms to all customers who are covered entities or business associates under HIPAA for use of such in-scope cloud services. In the BAA, Microsoft makes contractual assurances about data safeguarding, reporting (including breach notifications), data access in accordance with HIPAA and the HITECH Act, and many other important provisions. In addition, a HIPAA Assessment for Office 365 is available in Compliance Manager.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Azure Communications Service, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection, Access Online, Project Online, Office Services Infrastructure, Office 365 Customer Portal, Identity Manager, Service Encryption with Customer Key, Lockbox (Torus), Customer Lockbox, Griffin, Office 365 Microservices (including but not limited to Kaizala, ObjectStore, Sway, PowerPoint Online Document Service, Query Annotation Service, School Data Sync, Siphon, Speech, StaffHub, eXtensible Application Program)
GCC	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Azure Communications Service, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and

	Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection

29 HITRUST (USA)

The Health Information Trust Alliance (HITRUST) is an organization governed by representatives from the healthcare industry. HITRUST created and maintains the Common Security Framework (CSF), a certifiable framework to help healthcare organizations and their providers demonstrate their security and compliance in a consistent and streamlined manner. The CSF builds on HIPAA and the HITECH Act, and incorporates healthcare-specific security, privacy, and other regulatory requirements from existing frameworks such as PCI DSS, ISO 27001, and MARS-E.

HITRUST provides a benchmark—a standardized compliance framework, assessment, and certification process—against which cloud service providers and covered health entities can measure compliance. HITRUST offers three degrees of assurance, or levels of assessment: self-assessment, CSF validated, and CSF certified. Each level builds with increasing rigor on the one below it.

The Office 365 HITRUST CSF Assessment Report, the Office 365 HITRUST Letter of Certification, and the Office 365 HITRUST Customer Responsibility Matrix are available for download from the Service Trust Portal.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Delve, People Card, Teams, Office Service Infrastructure, Office 365 Customer Portal, Bing Services, Windows Ink, Activity Feed Service, Usage Reports

30 NEN 7510:2011 (Netherlands)

Many healthcare organizations in the Netherlands must perform periodic audits and demonstrate compliance with the NEN 7510 standard. When using Microsoft cloud services, some of the NEN 7510 controls for deployed applications are managed by Microsoft. Even though Microsoft is not subject to compliance with NEN 7510, Dutch healthcare organizations are seeking ways to demonstrate compliance with NEN 7510 when using cloud services. They need to determine if the cloud services they are using meet the requirements of NEN 7510.

Microsoft retained an independent, third-party auditing firm to analyze the extent to which current Microsoft's certifications and attestations (such as ISO 27001 and SOC 2 Type 2) cover the part of NEN 7510 for which Microsoft is responsible. The resulting NEN 7510 Coverage Report provides a mapping of these existing certifications and attestations to the controls listed in the NEN 7510 standard. Customers in the Dutch healthcare industry can use the report as a tool to help adopt Microsoft cloud services in a NEN 7510 compliant way. The report clearly demonstrates which NEN 7510 controls are covered by Microsoft and which controls remain to be covered by the customers.

Applicability	Services in scope
Office 365	Azure Information Protection, Bookings, Exchange Online, Exchange Online Protection, Flow, Kaizala, Microsoft Analytics, Microsoft Booking, Microsoft Graph, Planner, PowerApps, Microsoft StaffHub, Microsoft Stream, Teams, Microsoft To-

	Do for Web, MyAnalytics, Office 365 Cloud App Security, Office 365 Groups, Office 365 Video, Office Delve, OneDrive for Business, Power Apps, Power BI for Office 365, SharePoint Online, Skype for Business, Sway, Yammer Enterprise

31 PCI DSS

The Payment Card Industry (PCI) Data Security Standards (DSS) is a global information security standard designed to prevent fraud through increased control of credit card data. Organizations of all sizes must follow PCI DSS standards if they accept payment cards from the five major credit card brands — Visa, MasterCard, American Express, Discover, and the Japan Credit Bureau (JCB). Compliance with PCI DSS is required for any organization that stores, processes, or transmits payment and cardholder data.

Microsoft completed an annual PCI DSS assessment using Qualified Security Assessor (QSA), resulting in an Attestation of Compliance (AoC) available to the consumer. Microsoft is compliant under PCI DSS version 3.2 at Service Provider Level 1 (the highest volume of transactions — more than 6 million a year

Applicability	Services in scope
Office 365	SharePoint Online, OneDrive for Business (United States)

32 SOX (USA)

The Sarbanes-Oxley Act of 2002 (SOX) is a US federal law administered by the Securities and Exchange Commission (SEC). There is no SOX certification or validation for cloud service providers; however, Office 365 can help customers meet their obligations under SOX, which is heavily influenced by customer's internal processes especially when it comes to controls for financial reporting. Customers enquiring about Office 365 SOX compliance should review the Office 365 SOC 1 Type 2 attestation that is based on the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements 18 (SSAE 18) standard (see AT-C Section 105) and the International Standard on Assurance Engagements No. 3402 (ISAE 3402).

Applicability	Services in scope
Office 365	Augmentation Loop, Auto Alt Text, Azure Information Protection, Binary Conversion Services, Bookings, Document Item, Editor, Exchange Online, Flow, Forms, Information Protection, Insert Online Media, Insights, Kaizala, Microsoft Analytics, Microsoft Booking, Microsoft Graph, Planner, PowerApps, Microsoft Stream, Teams, Microsoft To-Do, MyAnalytics, Office 365 Cloud App Security, Office 365 Groups, Office 365 Video, Office Delve, OneDrive for Business, Power Apps, Power BI for Office 365, PowerPoint Designer, PowerPoint Online Document Service, SharePoint Online, Skype for Business, StaffHub, Sway, Web Rendering Service, Yammer Enterprise

Region / Country Specific

The following compliance offerings are specific to various regional and country laws and regulations. Some of these offerings are based on independent third-party certifications and attestations, whereas others provide contract amendments and guidance documentation to help customers meet their own compliance obligations.

33 Argentina PDPA

In accordance with the Argentine National Constitution, the Argentina Personal Data Protection Act 25,326 aims to protect personal information recorded in data files, registers, banks, and elsewhere to help protect the privacy of individuals, and also provide a right of access to the information that may be recorded about them. In a data transfer agreement available to customers, Microsoft contractually commits that Office 365 in-scope services have implemented the applicable technical and organizational security measures stated in Regulation 11/2006 of the Argentine Data Protection Authority. Moreover, Microsoft makes additional important commitments regarding notifications, auditing of our facilities, and use of subcontractors.

Applicability	Services in scope
Office 365	Azure Information Protection, Bookings, Exchange Online, Exchange Online Protection, Flow, Kaizala, Microsoft Analytics, Microsoft Booking, Microsoft Graph, Planner, PowerApps, Microsoft StaffHub, Microsoft Stream, Teams, Microsoft To-Do for Web, MyAnalytics, Office 365 Cloud App Security, Office 365 Groups, Office 365 Video, Office Delve, OneDrive for Business, Power Apps, Power BI for Office 365, SharePoint Online, Skype for Business, Sway, Yammer Enterprise

34 Australia IRAP PROTECTED

The Australian Cyber Security Center (ACSC) has certified Office 365 in-scope services for the processing of government data at the PROTECTED level in Microsoft Australian-based public cloud. The ACSC encourages adoption of a risk-managed approach with respect to the controls listed in the Australian Government Information Security Manual (ISM) and Protective Security Policy Framework (PSPF).

The ACSC intends to regularly communicate considerations when contemplating the use of Office 365 and other cloud-based services. Microsoft publishes all CCSL and IRAP guidance on an Australia specific page of the Service Trust Portal

Applicability	Services in scope
Office 365	Exchange Online, Exchange Online Protection, SharePoint Online, OneDrive for Business, Skype for Business, Teams, Office Online, Office Service Infrastructure, Office 365 Customer Portal, Forms, Planner, Whiteboard, Yammer

35 Europe EN 301 549

Accessibility requirements suitable for public procurement of ICT products and services in Europe (EN 301 549) is a set of standards for information and communications technologies (ICT) products and

services, including websites, software, and digital devices. EN 301 549 was published in 2014 by the European Telecommunications Standards Institute (ETSI) in response to a request from the European Commission and is intended for use in procurement by government and public-sector organizations.

Applicability	Services in scope
Office 365 GCC	See list of EN 301 459 reports for list of Microsoft products/services.

36 EU ENISA IAF

The European Network and Information Security Agency (ENISA) Information Assurance Framework (IAF) is a set of assurance criteria that organizations can review with cloud service providers to ensure they have sufficient protections in place around Customer Data. The IAF is intended to assess the risk of cloud adoption and reduce the assurance burden on cloud service providers. Office 365 aligns to the IAF by way of a self-assessment to the Cloud Security Alliance (CSA) STAR program. Office 365 maintains a STAR registry submission based on the Cloud Controls Matrix (CCM). The CCM maps to the IAF.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection, Azure Information Protection, Bookings, Exchange Online Protection, Kaizala, Microsoft Analytics, Microsoft Booking, Microsoft Graph, Microsoft StaffHub, Microsoft To-Do for Web, Office 365 Cloud App Security, Office 365 Groups, Office 365 Video, Sway, Yammer Enterprise

37 EU Model Clauses

European Union (EU) data protection law regulates the transfer of EU customer personal data to countries outside the European Economic Area (EEA), which includes all EU countries and Iceland, Liechtenstein, and Norway. Microsoft offers customers the EU Standard Contractual Clauses (EU Model Clauses) that provide specific guarantees around transfers of personal data for in-scope services. Microsoft provided its Standard Contractual Clauses to the EU's Article 29 Working Party for review and approval. The Article 29 Working Party includes representatives from the European Data Protection Supervisor, the European Commission, and each of the 28 EU data protection authorities (DPAs). The group determined that implementation of the provisions in Microsoft agreements was in line with their stringent requirements.

The EU Model Clauses ensure that any personal data leaving the EU will be transferred in accordance with EU data protection law and meet the requirements of the EU Data Protection Directive 95/46/EC. Microsoft makes the EU Model Clauses available to customers as described in the Online Services Terms.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365

Applicability	Services in scope
	Advanced Threat Protection, Azure Information Protection, Bookings, Exchange Online Protection, Kaizala, Microsoft Analytics, Microsoft Booking, Microsoft Graph, Microsoft StaffHub, Microsoft To-Do for Web, Office 365 Cloud App Security, Office 365 Groups, Office 365 Video, Sway, Yammer Enterprise

38 EU-US Privacy Shield

Microsoft and its controlled U.S. subsidiaries (Microsoft) comply with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Microsoft has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. Microsoft's participation in the Privacy Shield applies to all personal data that is subject to the Microsoft Privacy Statement and is received from the European Union, European Economic Area, and Switzerland. Microsoft will comply with the Privacy Shield Principles with respect to such personal data. More information is available from the EU-US Privacy Shield page.

Applicability	EU-U.S. Privacy Shield compliance
Microsoft	Microsoft and its controlled U.S. subsidiaries

39 EU GDPR

The General Data Protection Regulation (GDPR) is a European privacy law that became effective in May 2018. It imposes new rules on organizations that offer goods and services to people in the European Union (EU) or that collect and analyze personal data belonging to EU individuals. The GDPR requires that data controllers (such as organizations using Office 365) only use data processors (such as Microsoft) that provide sufficient guarantees to meet key requirements of the GDPR. Microsoft provides customers with a contractual commitment regarding the GDPR in the Online Services Terms (OST), which can be found in Attachment 4 to the OST, at the end of the document.

Microsoft provides tools and documentation to support customer's GDPR accountability including support for Data Subject Requests, Data Protection Impact Assessments, and Data Breach Notification, as described in Getting Started: Support for GDPR Accountability. Additional online documentation and white papers are available to help customers meet their own GDPR compliance obligations. A GDPR Assessment for Office 365 is also available in Compliance Manager.

Applicability	Services in scope
Office 365	All Online Services except Bing Maps Enterprise Platform, Bing Maps Mobile Asset Management Platform, Bing Search Services, LinkedIn Sales Navigator, Microsoft Azure Stack, Microsoft Genomics, and Visual Studio App Center, which are governed by the privacy and security terms in the applicable Online Service-specific Terms. Preview services are also excluded.

40 Japan CS Mark Gold

The Cloud Security Mark (CS Mark) is the first security standard for cloud service providers (CSPs) in Japan. It is based on ISO 27017, the international code of practice for cloud services information security controls. The CS Mark is accredited by the Japan Information Security Audit Association (JASA), a

nonprofit organization established by the Ministry of the Interior and the Ministry of Economy, Trade, and Industry to strengthen information security in Japan.

JASA developed the Authorized Information Security Audit System (AISAS), which specifies the audit of approximately 1,500 controls that needs to be performed by an independent auditor authorized by JASA. Office 365 completed a rigorous audit by a JASA-certified auditor and received CS Mark Gold accreditation for in-scope services. Customers can download the accreditation (in Japanese) from JASA web site.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection, Azure Information Protection, Bookings, Exchange Online Protection, Kaizala, Microsoft Analytics, Microsoft Booking, Microsoft Graph, Microsoft StaffHub, Microsoft To-Do for Web, Office 365 Cloud App Security, Office 365 Groups, Office 365 Video, Sway, Yammer Enterprise

41 Japan My Number Act

The My Number Act (Japanese and English) was enacted in 2013, and took effect in January 2016. It assigns a unique number—My Number that is also called the Social Benefits and Tax Number—to every resident of Japan, whether Japanese or foreign. The Personal Information Protection Commission has issued guidelines and Q&A (in Japanese) to ensure that companies properly handle and adequately protect My Number data as required by law.

While the responsibility and ownership of personal data is with our customers, per the Online Services Terms, Microsoft contractually commits that Office 365 in-scope cloud services have implemented technical and organizational security safeguards to help our customers protect individuals' privacy. These safeguards are based on established industry standards, such as ISO 27001 and SOC 2 Type 2.

Furthermore, Microsoft does not have standing access to My Number data stored in these in-scope cloud services, so companies do not need to supervise handling of data by Microsoft (as outlined in Q3-12). Nonetheless, companies are required to take appropriate safety measures to protect My Number data stored in the cloud (Q3-13).

Applicability	Services in scope
Office 365	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection, Azure Information Protection, Bookings, Exchange Online Protection, Kaizala, Microsoft Analytics, Microsoft Booking, Microsoft Graph, Microsoft StaffHub, Microsoft To-Do for Web, Office 365 Cloud App Security, Office 365 Groups, Office 365 Video, Sway, Yammer Enterprise

42 Netherlands BIR 2012

Organizations operating in the Netherlands government sector must perform periodic audits to demonstrate compliance with the Baseline Informatiebeveiliging Rijksdienst standard (BIR 2012). The BIR 2012 provides a standard framework based on ISO 27001. When using Office 365, some of the BIR 2012 controls for deployed applications are managed by Microsoft in line with the shared responsibility model in cloud computing. Even though Microsoft is not subject to compliance with BIR 2012, Dutch public sector organizations are seeking ways to demonstrate compliance with BIR 2012 when using Office 365. They need to determine if the services they are using meet the requirements of BIR 2012.

Microsoft retained an independent, third-party auditing firm to analyze the extent to which current Office 365 certifications and attestations (such as ISO 27001 and SOC 2 Type 2) cover the part of BIR 2012 that Microsoft is responsible for. The resulting BIR 2012 Coverage Report provides a mapping of these existing certifications and attestations to the controls listed in the BIR 2012 standard. Customers can use the report as a tool to help adopt Office 365 in a BIR 2012 compliant way. The report clearly demonstrates which BIR 2012 controls are covered by Microsoft and which controls remain to be covered by the customers. The Microsoft Cloud – Azure and Office 365 BIR-2012 Baseline Coverage report can be downloaded from the Service Trust Portal. Also available for download from the Service Trust Portal is the "Microsoft Cloud – Azure and Office 365 BIR 2012 Baseline Coverage User Guide" (in Dutch).

Applicability	Services in scope
Office 365	Azure Information Protection, Bookings, Exchange Online, Exchange Online Protection, Flow, Kaizala, Microsoft Analytics, Microsoft Booking, Microsoft Graph, Planner, PowerApps, Microsoft StaffHub, Microsoft Stream, Teams, Microsoft To-Do for Web, MyAnalytics, Office 365 Cloud App Security, Office 365 Groups, Office 365 Video, Office Delve, OneDrive for Business, Power Apps, Power BI for Office 365, SharePoint Online, Skype for Business, Sway, Yammer Enterprise

43 New Zealand Government CC Framework

To assist New Zealand government agencies in conducting consistent and robust due diligence on potential cloud solutions, the Government CIO has published "Cloud Computing: Information Security and Privacy Considerations" (Cloud Computing ISPC). This document contains more than 100 questions focused on data sovereignty, privacy, security, governance, confidentiality, data integrity, availability, and incident response and management.

To help agencies undertake their analysis and evaluation of Microsoft enterprise cloud services, Microsoft New Zealand has produced a series of documents showing how its enterprise cloud services address the questions set out in the Cloud Computing ISPC by linking them to the standards against which Microsoft cloud services are certified. These certifications are central to how Microsoft assures both public and private sector customers that its cloud services are designed, built, and operated to effectively mitigate privacy and security risks and address data sovereignty concerns.

Applicability	Services in scope
Office 365	Exchange Online, SharePoint Online, and Skype for Business. Note that Microsoft NZ has worked with the GCIO team to develop a reference

	architecture for integrating Exchange Online and SEEMail described in Office 365: SEEMail Integration and Reference Architecture.

44 Singapore MTCS Level 3

The Multi-Tier Cloud Security (MTCS) Standard for Singapore was prepared under the direction of the Information Technology Standards Committee (ITSC) of the Infocomm Media Development Authority of Singapore (IMDA). The ITSC promotes national programs to standardize IT and communications and facilitates Singapore's participation in international standardization activities.

The MTCS builds upon recognized international standards such as ISO 27001. It includes a total of 535 controls, and it addresses different levels of security, covering basic security in Level 1, more stringent governance and tenancy controls in Level 2, and reliability and resiliency for high-impact information systems in Level 3.

After a rigorous assessment conducted by the MTCS Certification Body, Office 365 was granted certification at Level 3. A Level 3 certification means that in-scope Office 365 services can host high-impact data for regulated organizations with the strictest security requirements. It's required for certain cloud solution implementations by the Singapore government. Office 365 MTCS certificate and MTCS cloud service provider self-disclosure can be downloaded from IMDA web site.

Applicability	Services in scope
Office 365	Exchange Online, SharePoint Online, Protection, Skype for Business, Teams, Delve, Loki, Office Online, Office Service Infrastructure, Office 365 Customer Portal

45 Spain DPA

The Spanish Data Protection Agency (Agencia Española de Protección de Datos – AEPD) has examined Microsoft Online Services Terms with specific focus on international data transfers and protection of personal data belonging to Spanish citizens. Following the assessment, the agency issued a resolution stating that Office 365 provides adequate protection for personal data to comply with Spanish Data Protection Law (Ley Orgánica de Protección de Datos – LOPD). The resolution covers the export of data to Microsoft Corporation in the United States and, through the EU Model Clauses provisions, the possibility of onward transfer to subcontractors in other countries where Microsoft operates. The resolution affirms Microsoft's commitment to helping Office 365 customers meet their LOPD compliance requirements.

Moreover, Microsoft has retained an independent third-party auditing firm in Spain to assess Office 365 compliance with LOPD. The resulting certificate and audit report (in Spanish) can be downloaded from the Service Trust Portal.

Applicability	Services in scope
Office 365	Office Online, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Delve, Azure Active Directory, Teams, Planner, Forms, PowerApps, Flow, Stream, Office Pro Plus, Security and Compliance Center, MyAnalytics, PowerBI, Advanced Compliance, Compliance Manager, Office 365 Advanced Threat Protection, Azure Information Protection, Bookings, Exchange Online Protection, Kaizala, Microsoft Analytics, Microsoft Booking, Microsoft

Applicability	Services in scope
	Graph, Microsoft StaffHub, Microsoft To-Do for Web, Office 365 Cloud App Security, Office 365 Groups, Office 365 Video, Sway, Yammer Enterprise

46 Spain ENS High

In 2007, the Spanish government enacted Law 11/2007, which established a legal framework to give citizens electronic access to public services. This law is the basis for the National Security Framework (Esquema Nacional de Seguridad – ENS), which is governed by Royal Decree (RD) 3/2010. The goal of the framework is to build trust in the provision of electronic services. The framework applies to all public organizations and government agencies in Spain that purchase cloud services, as well as to providers of information and communications technologies.

The framework establishes core policies and mandatory requirements that both government agencies and their service providers must meet. It defines a set of security controls, many of which align directly with ISO 27001. The sensitivity of the information—Low, Intermediate, or High—determines the security measures that must be applied to protect it. The framework prescribes an accreditation process that is voluntary for systems handling information of Low sensitivity, but mandatory for systems handling information at an Intermediate or High level of sensitivity. An audit is performed by an accredited independent auditor; the report is then reviewed as part of a certification process before risk-management controls are approved in the final accreditation step.

Office 365 has completed a rigorous assessment by an accredited independent auditor and has obtained an official statement of compliance indicating a Favorable ruling at the ENS High level for the final audit report. Customers can download the Office 365 ENS Certificate (in Spanish and in English) and Audit Assessment Report (in Spanish and in English) from the Service Trust Portal.

Applicability	Services in scope
Office 365	Exchange Online, SharePoint Online, Skype for Business, Exchange Online Protection, Office Online, Office 365 Office 365 Customer Portal, Office Service Infrastructure, MyAnalytics, MS Teams, Outlook Mobile

47 UK G-Cloud

Government Cloud (G-Cloud) is a UK government initiative to ease procurement of cloud services by government departments and promote government-wide adoption of cloud computing. G-Cloud comprises a series of framework agreements with cloud services suppliers (such as Microsoft), and a listing of their services in an online store—the Digital Marketplace. This approach enables public-sector organizations to compare and procure cloud services without having to do their own full review process. Inclusion in the Digital Marketplace requires a self-attestation of compliance, followed by a verification performed by the Government Digital Service (GDS) branch at its discretion.

The G-Cloud appointment process requires cloud service providers to self-certify and supply evidence in support of the UK National Cyber Security Centre (NCSC) 14 Cloud Security Principles. Every year, Microsoft prepares documentation and submits evidence to attest that its in-scope cloud services comply with the principles, giving potential G-Cloud customers an overview of its risk environment. A GDS accreditor then performs several random checks on the Microsoft assertion statement, samples the evidence, and makes a determination of compliance.

The appointment of Office 365 to the Digital Marketplace means that UK government agencies and partners can use in-scope services to store and process UK OFFICIAL government data, which comprises most government data.

Applicability	Services in scope
Office 365	Exchange Online, SharePoint Online, and Skype for Business

Frequently Asked Questions

1. **Why do the in-scope services vary for each regulation and standard?**
   Microsoft provides the most comprehensive offerings than other cloud service providers. To keep up with our broad compliance offerings across regions and industries, we include services in the scope of our assurance efforts based on the market demand, customer feedback, and product lifecycle. If a service is not included in the current scope of a specific compliance offering, your organization has the responsibility to assess the risks based on your compliance obligations and determine the way you process the data in that service. We continuously collect feedback from customers and work with regulators and auditors to expand our compliance coverage to meet your security and compliance needs.

2. **Do these compliance offerings represent my organization's usage of Office 365 compliant with the regulation or standard listed?**
   When you store your data in a SaaS application like Office 365, it's a shared responsibility between Microsoft and your organization to achieve compliance. Microsoft manages majority of the infrastructure controls including physical security, network controls, application level controls, etc., and your organization has the responsibility to manage access controls and protect your sensitive data. For examples, the Office 365 ISO 27001 certification demonstrates the compliancy of Microsoft's control framework. Building on that, your organization need to implement and maintain your own data protection controls to meet ISO 27001 requirements.

3. **Does Microsoft provide guidance for my organizations to implement appropriate controls when using Office 365?**
   In each section of the compliance offering, we summarize the resources you can leverage to implement your own controls. In most cases, you can find compliance guidance on Service Trust Portal > Trust Documents > Data Protection > Compliance Guides. For several regulations and standards, we provide you with recommended customer actions in Compliance Manager, a cross-Microsoft Cloud application that help your organization to meet complex compliance obligations when using Microsoft cloud services. You can learn more about Compliance Manager and Service Trust Portal in this whitepaper.