Compliance Framework for Industry Standards and Regulations for Office 365 and related Microsoft services

Published: May 2019

Introduction

We work hard to bring our customers the latest innovations in productivity with Office 365 and related Microsoft services. At the same time, we understand that compliance with standards and regulations, and the ability to use integrated tools to help meet compliance needs, are imperative and unwavering requirements for our customers.

To help customers with their compliance needs related to Office 365, we have created a compliance framework that is designed to give customers visibility into Office 365's compliance with global, regional and industry standards, and details how customers can control Office 365 services based on compliance needs.

Compliance Framework of Office 365 and Related Microsoft Services

Within this compliance framework, Microsoft classifies applications and services into four tiers. Each tier is defined by specific compliance commitments that must be met for an Office 365 service, or a related Microsoft service, to be listed in that tier.

Services in compliance categories C and D that have industry leading compliance commitments are enabled by default while services in categories A and B come with controls to enable or to disable these services for an entire organization.

A	B	C	D
Microsoft Cloud Services[1] Privacy and Security commitments	Microsoft Cloud Services Verified with International standards and terms	Microsoft Cloud Services Verified with International and Regional standards and terms	Microsoft Cloud Services Verified with International, Regional and Industry specific standards and terms
Strong Privacy and Security Commitments • No mining of customer data for advertising • No voluntary disclosure of customer data to law enforcement agencies • General Privacy and Security Terms of the Online Services Terms • FERPA	Strong Privacy and Security Commitments • ISO 27001 • ISO 27018 • EU Model Clauses (EUMC) • HIPAA Business Associate Agreement • Commitments included in Tier A	Strong Privacy and Security Commitments • SSAE 18 SOC 1 Report • SSAE 18 SOC 2 Report • Commitments included in Tiers A-B Contractual commitment to meet US and EU customer data residency requirements	Strong Privacy and Security Commitments • FedRAMP • IRS 1075 • FFIEC • HITRUST CSF Assurance Program Assessment • CSA STAR Self-Assessment • Australia IRAP • FISC (Japan) • Commitments included in Tiers A-C
Admin controls are available to enable or disable services in this tier	Admin controls are available to enable or disable services in this tier	Services in this tier may be enabled by default	Services in this tier are enabled by default

[1] Except as otherwise specified, this compliance framework does not apply to any client software component of a Microsoft cloud service because such a component runs on a customer's device and not in a Microsoft datacenter.

– Outlook Mobile for iOS and Android – Sunrise for iOS and Android –	– Workplace Analytics	– Azure Information Protection – Bookings – Flow – Kaizala[2] – Microsoft Dynamics 365 – Microsoft Forms – Microsoft Intune – Microsoft StaffHub – Microsoft To-Do for Web – Microsoft Whiteboard – MyAnalytics – Office 365 Video – Planner – Power Apps – Sway – Yammer Enterprise – Office 365 Cloud App Security	Office 365 for Enterprise, Education and Government plans that include – Access Online – Azure Active Directory – Exchange Online – Exchange Online Protection[3] – Microsoft Teams – Office 365 ProPlus[4] – Office Delve – Office Online – OneDrive for Business – Power BI – Power BI for Office 365 – Project Online – SharePoint Online – Skype for Business Online – Microsoft Stream

Maintaining our compliance commitments

Microsoft commits to the following principles with respect to the Office 365 compliance framework:

- A compliance tier can become stronger with more capabilities, but will not lose any of its current capabilities unless a particular standard or regulation becomes inapplicable.
  [Example: SOC 1 and SOC 2 may move from tier C to B but will not be dropped from C]
- A service or an application will not move to a tier with fewer compliance offerings (e.g., services or applications will not lose existing compliance capabilities unless a particular standard or regulation becomes inapplicable).
  [Example: Exchange Online will not move from D to C]
- Microsoft commits to keeping the compliance framework up to date to provide customers with the latest view of compliance across various Office 365 services and applications.
- Microsoft will provide the appropriate controls to enable customers to choose services in categories A and B based on their business need and appropriate consideration of risk. A guidance document provides customers with instructions to turn on or turn off services in categories A and B.

Frequently Asked Questions

To which Office 365 offerings does the Compliance Framework apply?

[2] Applies only to the customers' organizational groups managed through the Kaizala Pro admin portal

[3] Note that Exchange Online Protection is shown as Information Protection in the audit reports

[4] Office 365 ProPlus enables access to various cloud services, such as Roaming Settings, Licensing, and OneDrive consumer cloud storage, and may enable access to additional cloud services in the future. Roaming Settings and Licensing support the standards and terms in tier D. OneDrive consumer cloud storage does not, and other cloud services that are accessible through Office 365 ProPlus and that Microsoft may offer in the future also may not, support these standards and terms.

The Office 365 Compliance Framework applies to all Office 365 commercial, government and education online services offerings.

What information does this compliance framework provide?

This document communicates the tiered control framework and principles Microsoft uses to achieve compliance with sets of industry standards. It is not designed to communicate the compliance status of each service for each standard. For example, Microsoft Intune is FedRAMP-certified, but it's not specified in tier D because it's not IRAP-certified and has not been validated by outside assessors as meeting FISC guidelines yet. You can visit our Trust Center to get more details about the product compliance status and visit the Service Trust Portal to obtain product audit reports.

What does the Compliance Framework mean for customers of Office 365 in various geographies or industries?

A key commitment Microsoft makes to customers is transparency in service operations. With this view of compliance across the Microsoft cloud, customers can make informed decisions to enable services based on geography and industry regulations while considering their own business requirements.

How do customers control services or experiences that are enabled in their environment based on the compliance categories?

Another commitment Microsoft makes with respect to this framework is to provide appropriate controls for customers to use Office 365 based on their business needs and compliance requirements. Using the controls provided in the guidance document, customers can enable or disable services in A and B.