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

Published: September 2017

## 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.

## What's Changed

**Product changes:**

- Power BI is now in tier C.
- Azure Rights Management is now Azure Information Protection, which has broader offerings and is under tier C.
- Workplace Analytics was added to tier A.

**Tier changes:**

- General Privacy and Security Terms of the Online Services Terms and FERPA were added to tier A.
- HIPAA Business Associate Agreement was moved from tier C to tier B.
- Contractual commitment to meet US and EU customer data residency requirements was moved from tier D to tier C.

## Compliance Framework of Office 365 and Related Microsoft Services

Within this compliance framework, Microsoft classifies applications and services into four categories. Each category 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 category.

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 |

[1] 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.

| | | | |
|---|---|---|---|
| Strong Privacy and Security Commitments<br>• No mining of customer data for advertising<br>• No voluntary disclosure of customer data to law enforcement agencies<br>• General Privacy and Security Terms of the Online Services Terms<br>• FERPA | Strong Privacy and Security Commitments<br>• ISO 27001<br>• ISO 27018<br>• EU Model Clauses (EUMC)<br>• HIPAA Business Associate Agreement<br>• Commitments included in Tier A | Strong Privacy and Security Commitments<br>• SSAE 18 SOC 1 Report<br>• AT 101 SOC 2 Report<br>• Commitments included in Tiers A-B<br><br>Contractual commitment to meet US and EU customer data residency requirements | Strong Privacy and Security Commitments<br>• FedRAMP<br>• IRS 1075<br>• FFIEC<br>• HITRUST CSF Assurance Program Assessment<br>• CSA STAR Self-Assessment<br>• Australia IRAP<br>• FISC (Japan)<br>• Commitments included in Tiers A-C |
| Admin controls are available to enable or disable services in this category | Admin controls are available to enable or disable services in this category | Services in this category may be enabled by default | Services in this category are enabled by default |
| – Microsoft Graph<br>– Microsoft StaffHub<br>– Outlook Mobile for iOS and Android<br>– Sunrise for iOS and Android<br>– ToDo<br>– Workplace Analytics | | – Azure Information Protection<br>– Bookings<br>– Flow<br>– Microsoft Dynamics 365<br>– Microsoft Intune<br>– Microsoft Teams<br>– MyAnalytics<br>– Office 365 Video<br>– Planner<br>– Power Apps<br>– Power BI<br>– Power BI for Office 365<br>– Sway<br>– Yammer Enterprise<br>– Office 365 Cloud App Security | Office 365 for Enterprise, Education and Government plans that include<br>– Access Online<br>– Azure Active Directory<br>– Exchange Online<br>– Exchange Online Protection<br>– Office 365 ProPlus[2]<br>– Office Delve<br>– Office Online<br>– OneDrive for Business<br>– Project Online<br>– SharePoint Online<br>– Skype for Business Online |

## Maintaining our compliance commitments

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

- A compliance category 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 category C to B but will not be dropped from C]

[2] 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 category 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.

- A service or an application will not move to a category 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?**

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

**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.