ISO/IEC 27017:2015 Code of Practice for Information Security Controls

Microsoft cloud services have implemented this code of practice for information security controls.

Microsoft and ISO/IEC 27017

ISO/IEC 27017 is unique in providing guidance for both cloud service providers (CSPs) and cloud service customers. It also provides cloud service customers with practical information on what they should expect from CSPs. Customers can benefit directly from ISO/IEC 27017 by ensuring they understand the shared responsibilities in the cloud.

Microsoft in-scope cloud services

- Azure and Azure Government
  Learn more
- Cloud App Security
- Dynamics 365
  Learn more
- Flow cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Genomics
- Graph
- Intune
- Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense
  Learn more
- PowerApps cloud service either as a standalone service or in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or in an Office 365 branded plan or suite

Audits, reports, and certificates

Microsoft cloud services are audited once a year for the ISO/IEC 27017:2015 code of practice as part of the certification process for ISO/IEC 27001:2013.

- Azure ISO 27017 Certificate of Registration
- ISO/IEC 27017:2015 certificate for Azure, Intune, and Power BI
- Azure ISO 27017 Audit Report
- Azure ISO 27017 Statement of Applicability
- Office 365 ISO 27001, 27018, and 27017 Audit Assessment Report

About ISO/IEC 27017

The ISO/IEC 27017:2015 Code of practice for information security controls 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/IEC 27002:2013. It can also be used by CSPs 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 referring to clauses 5 to 18 in ISO/IEC 27002: 2013 for controls, implementation guidance, and other information. Specifically, this standard provides guidance on 37 controls in ISO/IEC 27002, and it also features 7 new controls that are not duplicated in ISO/IEC 27002. These new controls address the following important areas:

- Shared roles and responsibilities within a cloud computing environment
- Removal and return of cloud service customer assets upon contract termination
- Protection and separation of a customer's virtual environment from that of other customers
- Virtual machine hardening requirements to meet business needs
- Procedures for administrative operations of a cloud computing environment
- Enabling customers to monitor relevant activities within a cloud computing environment
- Alignment of security management for virtual and physical networks

Frequently asked questions

To whom does the standard apply?

This code of practice provides controls and implementation guidance for both CSPs and cloud service customers. It is structured in a format similar to ISO/IEC 27002:2013.

Can I use the ISO/IEC 27017 compliance of Microsoft services in my organization's certification process?

Yes. If your business is seeking certification for implementations deployed on any Microsoft in-scope enterprise cloud services, you can use relevant certifications of Microsoft services in your compliance assessment. However, you are responsible for engaging an assessor to evaluate your implementation for compliance, and for the controls and processes within your own organization.

How can I get copies of the applicable audit reports?

The Service Trust Portal provides independent, third-party audit reports and other related documentation. You can use the portal to download and review this documentation for assistance with your own regulatory requirements.

Additional resources

- Microsoft Online Services Terms