

ISO/IEC 27001:2013 Information Security Management Standards

Article • 05/19/2023

ISO/IEC 27001 overview

The International Organization for Standardization (ISO) is an independent nongovernmental organization and the world's largest developer of voluntary international standards. The International Electrotechnical Commission (IEC) is the world's leading organization for the preparation and publication of international standards for electrical, electronic, and related technologies.

Published under the joint ISO/IEC subcommittee, the ISO/IEC 27000 family of standards outlines hundreds of controls and control mechanisms to help organizations of all types and sizes keep information assets secure. These global 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/IEC 27001 is a security standard that formally specifies an Information Security Management System (ISMS) that is intended to bring information security under explicit management control. As a formal specification, it mandates requirements that define how to implement, monitor, maintain, and continually improve the ISMS. It also prescribes a set of best practices that include documentation requirements, divisions of responsibility, availability, access control, security, auditing, and corrective and preventive measures. Certification to ISO/IEC 27001 helps organizations comply with numerous regulatory and legal requirements that relate to the security of information.

Microsoft and ISO/IEC 27001

The international acceptance and applicability of ISO/IEC 27001 is the key reason why certification to this standard is at the forefront of Microsoft's approach to implementing and managing information security. Microsoft's achievement of ISO/IEC 27001 certification points up its commitment to making good on customer promises from a business, security compliance standpoint. Currently, both Azure Public and Azure Germany are audited once a year for ISO/IEC 27001 compliance by a third-party accredited certification body, providing independent validation that security controls are in place and operating effectively.

Learn about the benefits of ISO/IEC 27001 on the Microsoft Cloud: [Download the ISO/IEC 27001:2013](#) ↗ .

Microsoft in-scope cloud platforms & services

- Azure, Azure Government, and Azure Germany
- Azure DevOps Services
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- Dynamics 365, Dynamics 365 Government, and Dynamics 365 Germany
- Microsoft Graph
- Microsoft Healthcare Bot
- Intune
- [Microsoft Managed Desktop](#)
- Power Automate (formerly Microsoft Flow) cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense
- Office 365 Germany
- OMS Service Map
- PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

- Power BI Embedded
- Power Virtual Agents
- [Microsoft Professional Services](#) 
- Microsoft Stream
- Microsoft Threat Expert
- Microsoft Translator
- Microsoft Viva Topics
- Windows 365

Azure, Dynamics 365, and ISO 27001

For more information about Azure, Dynamics 365, and other online services compliance, see the [Azure ISO 27001:2013 offering](#).

Office 365 and ISO 27001

Office 365 environments

Microsoft Office 365 is a multi-tenant hyperscale cloud platform and an integrated experience of apps and services available to customers in several regions worldwide. Most Office 365 services enable customers to specify the region where their customer data is located. Microsoft may replicate customer data to other regions within the same geographic area (for example, the United States) for data resiliency, but Microsoft will not replicate customer data outside the chosen geographic area.

This section covers the following Office 365 environments:

- **Client software (Client):** commercial client software running on customer devices.
- **Office 365 (Commercial):** the commercial public Office 365 cloud service available globally.

- **Office 365 Government Community Cloud (GCC):** the [Office 365 GCC cloud service](#) is available for United States Federal, State, Local, and Tribal governments, and contractors holding or processing data on behalf of the US Government.
- **Office 365 Government Community Cloud - High (GCC High):** the [Office 365 GCC High cloud service](#) 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.
- **Office 365 DoD (DoD):** the [Office 365 DoD cloud service](#) 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.

Use this section to help meet your compliance obligations across regulated industries and global markets. To find out which services are available in which regions, see the [International availability information](#) and the [Where your Microsoft 365 customer data is stored](#) article. For more information about Office 365 Government cloud environment, see the [Office 365 Government Cloud](#) article.

Your organization is wholly responsible for ensuring compliance with all applicable laws and regulations. Information provided in this section does not constitute legal advice and you should consult legal advisors for any questions regarding regulatory compliance for your organization.

Office 365 applicability and in-scope services

Use the following table to determine applicability for your Office 365 services and subscription:

Applicability	In-scope services
Commercial	Access Online, Azure Active Directory, Azure Communications Service, Compliance Manager, Customer Lockbox, Delve, Exchange Online, Exchange Online Protection, Forms, Griffin, Identity Manager, Lockbox (Torus), Microsoft Defender for Office 365, Microsoft Teams, Microsoft Viva Topics, MyAnalytics, Office 365 Advanced Compliance add-on, Office 365 Customer Portal, Office 365 Microservices (including but not limited to Kaizala, ObjectStore, Sway, Power Automate,





Applicability	In-scope services
	PowerPoint Online Document Service, Query Annotation Service, School Data Sync, Siphon, Speech, StaffHub, eXtensible Application Program), Office 365 Security & Compliance Center, Office Online, Office Pro Plus, Office Services Infrastructure, OneDrive for Business, Planner, PowerApps, Power BI, Project Online, Service Encryption with Microsoft Purview Customer Key, SharePoint Online, Skype for Business, Stream
GCC	Azure Active Directory, Azure Communications Service, Compliance Manager, Delve, Exchange Online, Forms, Microsoft Defender for Office 365, Microsoft Teams, Microsoft Viva Topics, MyAnalytics, Office 365 Advanced Compliance add-on, Office 365 Security & Compliance Center, Office Online, Office Pro Plus, OneDrive for Business, Planner, PowerApps, Power Automate, Power BI, SharePoint Online, Skype for Business, Stream
GCC High	Azure Active Directory, Azure Communications Service, Exchange Online, Forms, Microsoft Defender for Office 365, Microsoft Teams, Office 365 Advanced Compliance add-on, Office 365 Security & Compliance Center, Office Online, Office Pro Plus, OneDrive for Business, Planner, PowerApps, Power Automate, Power BI, SharePoint Online, Skype for Business
DoD	Azure Active Directory, Azure Communications Service, Exchange Online, Forms, Microsoft Defender for Office 365, Microsoft Teams, Office 365 Advanced Compliance add-on, Office 365 Security & Compliance Center, Office Online, Office Pro Plus, OneDrive for Business, Planner, Power BI, SharePoint Online, Skype for Business

Office 365 audits, reports, and certificates

Office 365 cloud services are audited at least annually against the ISO 27001:2013 standard.

- [Office 365—Global and Germany ISO 27001: Information Security Management Standards Certificate](#) 

Office 365 assessments and reports

- [Office 365: ISO 27001, 27018, and 27017 Audit Assessment Report](#) 
- [Office 365: ISO 27001, 27018, and 27017 Statement of Authority \(SOA\)](#) 
- [Office 365: Information Security Management System \(ISMS\)—Statement Of Applicability for Security and Privacy](#) 
- [Office 365 Germany: ISO 27001, 27017, and 27018 Audit Assessment Report](#) 

Frequently asked questions

Why is Office 365 compliance with ISO/IEC 27001 important?

Compliance with these standards, confirmed by an accredited auditor, demonstrates that Microsoft uses internationally recognized processes and best practices to manage the infrastructure and organization that support and deliver its services. The certificate validates that Microsoft has implemented the guidelines and general principles for initiating, implementing, maintaining, and improving the management of information security.

Where can I get the ISO/IEC 27001 audit reports and scope statements for Office 365 services?

The [Service Trust Portal](#) provides independently audited compliance reports. You can use the portal to request reports so that your auditors can compare Microsoft's cloud services results with your own legal and regulatory requirements.

Are annual tests run for Office 365 infrastructure failures?

Yes. The annual ISO/IEC 27001 certification process for the Microsoft Cloud Infrastructure and Operations group includes an audit for operational resiliency. To view the latest certificate, select the link below.

- Microsoft 365 and Office 365 certificate: [ISO/IEC 27001:2013 certificate for Microsoft Cloud Infrastructure and Operations](#) ↗

Where do I start my organization's own ISO/IEC 27001 compliance effort?

Adopting ISO/IEC 27001 is a strategic commitment. As a starting point, consult the [ISO/IEC 27000 Directory](#) ↗.

Can I use the ISO/IEC 27001 compliance of Office 365 services in my organization's certification?

Yes. If your business requires ISO/IEC 27001 certification for implementations deployed on Microsoft services, you can use the applicable certification in your compliance assessment. You are responsible, however, for engaging an assessor to evaluate the controls and processes within your own organization and your implementation for ISO/IEC 27001 compliance.

Use Microsoft Purview Compliance Manager to assess your risk

[Microsoft Purview Compliance Manager](#) is a feature in the [Microsoft Purview compliance portal](#) to help you understand your organization's compliance posture and take actions to help reduce risks. Compliance Manager has a pre-built assessment for this regulation for Enterprise E5 customers. Find the template for building the assessment in the [assessment templates](#) page in Compliance Manager. Learn how to [build assessments in Compliance Manager](#).

Resources

- [Mapping Microsoft Cyber Offerings to: NIST Cybersecurity \(CSF\), CIS Controls, and ISO27001:2013 Frameworks](#) [↗](#)
- [The ISO/IEC 27000 Directory](#) [↗](#)
- [ISO/IEC 27001: 2013 standard](#) [↗](#) (for purchase)
- [Microsoft sets a high bar for information security](#) [↗](#) (BSI case study)
- [Microsoft Common Controls Hub Compliance Framework](#) [↗](#)
- [Microsoft Online Services Terms](#) [↗](#)
- [Microsoft Cloud for Government](#) [↗](#)