Service Organization Controls (SOC) 1, 2, and 3 Reports

Microsoft cloud services comply with Service Organization Controls standards for operational security.

Microsoft and SOC 1, 2, and 3 Reports

Microsoft covered cloud services are audited at least annually against the SOC reporting framework by independent third-party auditors. The audit for Microsoft cloud services covers controls for data security, availability, processing integrity, and confidentiality as applicable to in-scope trust principles for each service.

Microsoft has achieved SOC 1 Type 2, SOC 2 Type 2, and SOC 3 reports. In general, the availability of SOC 1 and SOC 2 reports is restricted to customers who have signed nondisclosure agreements with Microsoft; the SOC 3 report is publicly available.

Microsoft in-scope cloud services

Covered services for SOC 1, SOC 2, and SOC 3 Reports

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

Covered services for SOC 1 and SOC 2 Reports

- Azure DevOps
- Dynamics 365 and Dynamics 365 U.S. Government
  Learn more
- Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense. Yammer has achieved a SOC 2 report.
  Learn more
- Office 365 Germany

Audits, reports and certificates

Microsoft cloud services are audited at least annually against SOC 1 (SSAE18, ISAE 3402) and SOC 2 (AT Section 101) standards.

Azure, Cloud App Security, Flow, Graph, Intune, Power BI, PowerApps, Stream, and Microsoft Datacenters

- Azure and Azure Government SOC 1 Type 2 Report and Azure and Azure Government SOC 2 Type 2 Report
- Azure and Azure Government SOC 3 Report
- For Azure DevOps ONLY: Email Azure DevOps for its SOC 1 and SOC 2 reports.

Dynamics 365

- Dynamics 365 SOC 1 Type 2 Report and Dynamics 365 SOC 2 AT 101 Type II Audit Report
- See bridge letters and additional audit reports

Office 365

- Office 365 SOC 1 SSAE 16 Type II Audit Report and Office 365 SOC 2 AT 101 Type II Audit Report
- Office 365 Customer Lockbox SOC 1 SSAE 16 Audit Report
- See bridge letters and additional audit reports

How to implement

- **SOC Toolkit for Service Organizations**
  Get help understanding SOC reporting processes to start your organization's own compliance effort.
  Learn more

About SOC 1, 2, and 3 Reports

Increasingly, businesses outsource basic functions such as data storage and access to applications to cloud service providers (CSPs) and other service organizations. In response, the American Institute of Certified Public Accountants (AICPA) has developed the Service Organization Controls (SOC) framework, a standard for controls that safeguard the confidentiality and privacy of information stored and processed in the cloud. This aligns with the International Standard on Assurance Engagements (ISAE), the reporting standard for international service organizations.

Service audits based on the SOC framework fall into two categories—SOC 1 and SOC 2—that apply to in-scope Microsoft cloud services.

- A SOC 1 audit, intended for CPA firms that audit financial statements, evaluates the effectiveness of a CSP's internal controls that affect the financial reports of a customer using the provider's cloud services. The Statement on Standards for Attestation Engagements (SSAE 18) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402) are the standards under which the audit is performed, and is the basis of the SOC 1 report.
- A SOC 2 audit gauges the effectiveness of a CSP's system based on the AICPA Trust Service Principles and Criteria. An Attest Engagement under Attestation Standards (AT) Section 101 is the basis of SOC 2 and SOC 3 reports.

At the conclusion of a SOC 1 or SOC 2 audit, the service auditor renders an opinion in a SOC 1 Type 2 or SOC 2 Type 2 report, which describes the 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.

Auditors can also create a SOC 3 report—an abbreviated version of the SOC 2 Type 2 audit report—for users who want assurance about the CSP's controls but don't need a full SOC 2 report. A SOC 3 report can be conferred only if the CSP has an unqualified audit opinion for SOC 2.

Frequently asked questions

- **How often are Azure SOC reports issued?**
  SOC reports for Azure, Cloud App Security, Flow, Graph, Intune, Power BI, PowerApps, Stream, and Microsoft Datacenters are based on a rolling 12-month run window (audit period) with new reports issued quarterly. The increased audit frequency provides more timely audit period coverage through a SOC report which provides greater assurance by an external auditor when compared to a bridge letter.
- **Do I need to conduct my own audit of Microsoft datacenters?**
  No. Microsoft shares the independent audit reports and certifications with customers so that they can verify Microsoft compliance with its security commitments.
- **Can I use Microsoft compliance in my organization's certification process?**
  Yes. When you migrate your applications and data to covered Microsoft cloud services, you can build on the audits and certifications that Microsoft holds. The independent reports attest to the effectiveness of controls that Microsoft has implemented to help maintain the security and privacy of your data.

Additional resources

- Better protect your data by using Microsoft cloud services
- Service Organization Control (SOC) Reports
- SSAE 16 Auditing Standard
- ISAE 3402 Standard
- Microsoft Online Services Terms
- Microsoft Cloud for Government