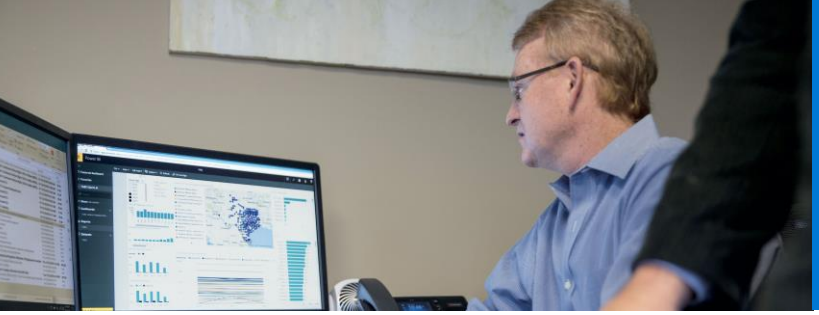

Sarbanes-Oxley Act of 2002 (SOX)
United States

Financial services firms can leverage Microsoft compliance reports to address their compliance with the Sarbanes-Oxley Act.

Microsoft and SOX

Microsoft cloud services customers subject to compliance with the US Sarbanes-Oxley Act (SOX) can leverage the SOC 1 Type 2 attestation that Microsoft received from an independent auditing firm when addressing their own SOX compliance obligations. This attestation is appropriate for reporting on internal controls over financial reporting.

Even though there is no SOX certification or validation for cloud service providers, Microsoft can help customers meet their SOX obligations. For example, SOX requires internal controls for the preparation and review of financial statements, especially controls that affect the accuracy, completeness, effectiveness, and public disclosure of material changes related to financial reporting. To help companies, Microsoft maintains a SOC 1 Type 2 attestation appropriate for reporting on such controls across a broad portfolio of services that can be used to build a wide range of applications. It is based on the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements 18 (SSAE 18) and the International Standard on Assurance Engagements No. 3402 (ISAE 3402). (This attestation replaced SAS 70.)

The audit report, produced by a third-party auditing firm, attests that Microsoft controls were designed appropriately, in operation on a specified date, and operating effectively over a specified time period. Customers can review the reports to learn about Microsoft control objectives and the effectiveness of its controls, as well as get access to complementary controls.

To further help Microsoft Azure clients address their SOX obligations, Microsoft has published *Azure Guidance for Sarbanes-Oxley*. This paper provides migration best practices, including the implications of complying with SOX, and draws on internal experience migrating SOX-relevant applications—Microsoft Treasury and Microsoft Finance—to Azure.

Note, however, that at Microsoft we share the responsibility of compliance with our customers. We supply the specifics about our compliance programs, which you can verify by requesting detailed audit results from the certifying third parties. Ultimately, however, it is up to you to determine whether our services comply with the specific laws and regulations applicable to your business. For example, there are SOX-related security controls, such as user access to cloud resources, that are your responsibility: your organization must develop appropriate auditing of these controls as part of your SOX compliance.

Microsoft in-scope cloud services

- Azure
  Learn more
- Dynamics 365
  Learn more
- Intune
- Office 365
  Learn more
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

Audits, reports, and certificates

SOC 1 Type 2 reports for:

- Azure and Power BI
- Dynamics 365
- Office 365

How to implement

- **Azure guidance for SOX**
  Learn how to leverage Azure compliance reports when addressing your SOX compliance obligations.
  Learn more
- **Risk Assessment & Compliance Guide**
  Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
  Learn more
- **Financial use cases**
  Case overviews, tutorials, and other resources to build Azure solutions for financial services.
  Learn more
- **Financial services regulation**
  Compliance map of key US regulatory principles for cloud computing and Microsoft online services.
  Learn more

About SOX

The Sarbanes-Oxley Act of 2002 is a US federal law administered by the Securities and Exchange Commission (SEC). Among other directives, SOX requires publicly traded companies to have proper internal control structures in place to validate that their financial statements accurately reflect their financial results.

The SEC does not define or impose a SOX certification process; instead, it provides broad guidelines for the companies it regulates to determine how to comply with SOX reporting requirements.

Frequently asked questions

How can I leverage Microsoft SOX compliance to facilitate my organization's compliance process?

When you migrate your applications and data to covered Microsoft cloud services, you can build on the attestations and certifications that Microsoft holds. Independent auditor reports attest to the effectiveness of controls that Microsoft has implemented to help maintain the security and privacy of your data. However, you are wholly responsible for ensuring your organization's compliance with all applicable laws and regulations.

Additional resources

Microsoft Financial Services Compliance Program

Financial services compliance in Azure

Microsoft business cloud services and financial services

Shared responsibilities for cloud computing