Federal Financial Institutions Examination Council (FFIEC) United States

Microsoft helps financial services clients comply with the audit requirements of the Federal Financial Institutions Examination Council.

Microsoft and the FFIEC

Microsoft Azure, Microsoft Power BI, and Microsoft Office 365 are built to meet the stringent requirements of providing cloud services for financial services institutions. As part of our support, we offer guidance to help you comply with FFIEC audit requirements for information technology and the ability to leverage Azure SOC attestations when pursuing your FFIEC compliance obligations.

To help financial institution clients meet their FFIEC compliance requirements with Azure, Microsoft has developed the:

- Cloud Security Diagnostic Tool to help you more efficiently conduct a risk assessment of Azure services. The tool (an Excel spreadsheet) features 19 information security domains (such as network and system security and information and risk management) that track the requirements of financial services regulations and other relevant standards, as well as the FFIEC IT Examination Handbooks. The tool explains how Azure complies with each requirement applicable to technology service providers (TSPs).
- Azure Security and Compliance Blueprint for FFIEC Regulated Services Workloads, a companion to the diagnostic tool. It offers guidance on the use of Azure cloud services and considerations for customer compliance with FFIEC requirements and risk assessment guidelines.

To further help you comply with FFIEC requirements, Microsoft cloud services provide SOC attestation reports produced by an independent CPA firm. For example, the SOC 1 Type 2 attestation is based on the AICPA SSAE 18 standard (see AT-C Section 105) that replaced SAS 70, and is appropriate for reporting on certain controls for financial reporting. The SOC reports include the auditor's opinion on the effectiveness of Microsoft controls in achieving the related control objectives during the specified monitoring period. Financial institutions can leverage this formal audit when pursuing FFIEC-specific compliance obligations for assets deployed on Azure, Power BI, and Office 365.

Microsoft in-scope cloud services

- Azure
  Learn more
- Intune
- Office
  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

- Azure and Office 365 SOC attestation reports

How to implement

- **Cloud Security Diagnostic Tool**
  Get help to conduct a more efficient risk assessment of Azure services.
  Learn more
- **Azure FFIEC Blueprint**
  Supportive solutions for building FFIEC-compliant workloads in Azure.
  Learn more

May 2019

Microsoft

- **Risk Assessment & Compliance Guide**
  Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
  Learn more
- **Financial use cases**
  Use 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 the FFIEC

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body comprising five banking regulators that is responsible for US federal government examinations of financial institutions in the United States. The FFIEC Examiner Education Office publishes IT Examination Handbooks intended for field examiners from FFIEC member agencies.

The FFIEC Audit IT Examination Handbook contains guidance for these examiners to assess the quality and effectiveness of IT audit programs of both financial institutions and TSPs. Specifically, it includes mention of SOC 1, SOC 2, and SOC 3 attestation reports of the American Institute of Certified Public Accountants (AICPA) as examples of independent audit reports. However, the FFIEC recommends that financial institutions not rely solely on the information contained in these reports, but also use verification and monitoring procedures discussed in detail in the FFIEC Outsourcing Technology Services IT Examination Handbook.

Frequently asked questions

Can I use Microsoft compliance with SOC standards to meet the FFIEC compliance obligations for my institution?

To help you meet these obligations, Microsoft supplies the specifics about our compliance with SOC standards as described above. However, ultimately, it is up to you to determine whether our services comply with the specific laws and regulations applicable to your institution. The FFIEC also advises that “users of audit reports or reviews should not rely solely on the information contained in the report to verify the internal control environment of the TSP. They should use additional verification and monitoring procedures as discussed more fully in the Outsourcing Technology Booklet of the FFIEC IT Examination Handbook.”

Additional resources

- Compliance Map of Cloud Computing and Regulatory Principles in the US
- Microsoft Financial Services Compliance Program
- Financial services compliance in Azure
- Microsoft business cloud services and financial services
- Shared responsibilities for cloud computing