Title 23 New York Codes, Rules, and Regulations Part 500 (23 NYCRR 500)

Microsoft has prepared a guide to explain how Azure, Office 365, and Power BI can help financial institutions comply with 23 NYCRR 500 requirements.

Microsoft and Title 23 NYCRR Part 500

Microsoft provides a comprehensive guide, Microsoft Cloud Services: Supporting Compliance with NYDFS Cybersecurity Requirements, for financial services regulated under Title 23 NYCRR Part 500. It explains in depth how Microsoft Azure and Azure DevOps, Microsoft Office 365, and Microsoft Power BI cloud services support compliance with the requirements. Financial institutions that seek to operate in the global financial center of New York must meet them, so compliance is critical for many institutions.

The New York regulations require each financial institution to:

- **Develop and maintain a robust cybersecurity program,** starting with an assessment of the institution's specific risk profile and then designing a program that addresses it. The Microsoft Cloud Financial Services Compliance Program was specifically created to help financial services assess the risks of using Microsoft cloud services. It includes direct engagement with our engineers and corporate risk officers and access to our compliance and security experts.
- **Implement a comprehensive cybersecurity policy** that addresses information security, data governance and classification, access controls, business continuity, and the like. Microsoft offers guidance for developing this policy with in-depth information about our certifications and risk assessments; business continuity and disaster recovery metrics; and diagnostics for logging and auditing.
- **Designate a chief information security officer** (CISO) to manage the cybersecurity program and enforce policy. To help your CISO, Microsoft provides in-depth cybersecurity information about Microsoft cloud deployments through Azure Security Center, Office 365 Advanced Threat Analytics, and Power BI Security.
- **Monitor and test the effectiveness of its cybersecurity program.** Microsoft provides information from audits of its cybersecurity practices that include continuous monitoring, periodic penetration testing, and vulnerability assessments. Customers can conduct their own tests without advance permission from Microsoft.
- **Maintain an audit trail.** Built-in audit functionalities of Azure, Office 365, and Power BI generate information that can be used to reconstruct financial transactions and develop audit trail information.
- **Limit access to information systems that contain nonpublic information.** Azure, Office 365, and Power BI offer a role-based access control (RBAC) process native to each service, strict security and access requirements for every Microsoft administrator, and audits of every request for elevated access privileges.
- **Institute procedures to assess and test the security of externally developed applications.** For developers using Visual Studio, Security Rules for managed code can help ensure that application cybersecurity threats are detected and mitigated before the code is deployed.
- **Use periodic risk assessments to design and enhance cybersecurity programs.** For customers, Microsoft aggregates information about security threats, provides roadmaps of change management, and regularly updates information about subcontractors. Microsoft also regularly conducts risk assessments of its own services, the results of which are available to customers.
- **Use qualified personnel to manage cybersecurity risks and oversee cybersecurity functions.** Microsoft employs stringent procedures for our employee access to your customer data. If we hire subcontractors, we remain responsible for service delivery, and ensure that subcontractors fully comply with Microsoft privacy and security commitments, including requirements for handling sensitive data, background checks, and non-disclosure agreements.
- **Implement data retention and deletion policies and procedures.** You can always access and extract your customer data stored in Azure, Office 365, and Power BI.

- **Implement policies and procedures to ensure the security of information held by third-party service providers.** Azure, Office 365, and Power BI make multifactor authentication available for all inbound connections to company networks; implement controls, including encryption, to protect nonpublic information in transit over external networks and at rest; and offer Microsoft Online Services Terms that provide for customer notification, incident investigation, and risk mitigation for security incidents.
- **Monitor the activity of authorized users, detect unauthorized access, and offer regular cybersecurity awareness training to employees.** Azure, Office 365, and Power BI include outside-in monitoring to raise alerts about incidents, and extensive diagnostics for logging and auditing. Microsoft Virtual Academy offers online training that covers the cybersecurity of Microsoft cloud services.
- **Develop plans to respond to and recover from cybersecurity incidents.** Microsoft helps you prepare for cybersecurity incidents using a defensive strategy to detect, predict, and prevent security breaches before they occur. When developing your own plans, draw on our incident management plan for responding to cybersecurity breaches.

Microsoft in-scope cloud services

- Azure and Azure DevOps: 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

How to implement

- **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 Title 23 NYCRR Part 500

In response to the significant and ever-increasing threats to the cybersecurity of information and financial systems, in 2017, the State of New York Department of Financial Services imposed a new set of cybersecurity requirements on financial institutions that are licensed or authorized to do business in the state. This regulation—Title 23 New York Codes, Rules, and Regulation Part 500: Cybersecurity Requirements for Financial Services Companies—is designed to protect customer data and the information technology systems of financial institutions such as state-chartered, private, and international banks, mortgage brokers, and insurance companies.

Frequently asked questions

What institutions are covered under this regulation?

Consult the New York Department of Financial Services Who We Supervise to determine whether your institution is governed by this regulation.

Additional resources

Supporting Compliance with NYDFS Cybersecurity Requirements

FAQs: 23 NYCRR Part 500–Cybersecurity

Financial services compliance in Azure

Microsoft business cloud services and financial services

Shared responsibilities for cloud computing