NYDFS 23 NYCRR 500: Cybersecurity Compliance Guide for FinTech

Compliance Guide for Financial Technology

Prepared by Jacobian Engineering

Updated: 2026-02-09

This document is for educational purposes and does not constitute legal advice.

Executive Summary

NYDFS 23 NYCRR Part 500 is a cybersecurity regulation issued by the New York State Department of Financial Services. For covered entities, it sets minimum cybersecurity program requirements, governance expectations, and incident reporting obligations. For many FinTech organizations, the regulation shows up through direct coverage, through an affiliated regulated entity, or through bank partner requirements.

This guide explains Part 500 in a practical way. It focuses on what the regulation expects, what evidence is typically needed, and how to build an operating routine that supports ongoing compliance.

What NYDFS Part 500 covers and why it exists

NYDFS enacted Part 500 to establish cybersecurity requirements for financial services organizations under its supervision. The regulation emphasizes governance, risk-based controls, and accountability. It also requires covered entities to provide periodic certifications and to report certain cybersecurity events.

Part 500 is often treated as a checklist, but successful programs treat it like a risk management framework. The regulation expects controls to be designed around your risks and business model, and it expects leadership involvement through defined roles and reporting.

Organizations commonly impacted

- **Banks and insurance organizations:** Covered entities regulated by NYDFS.
- **FinTechs with regulated relationships:** Vendors supporting covered entities may be required to meet comparable expectations.
- **Organizations operating in New York:** If you offer regulated services in New York, confirm whether you fall under NYDFS supervision.

Key control areas in NYDFS Part 500

The regulation includes multiple requirements, but most map to a set of recurring control areas. A practical approach is to assign an owner to each area and define what evidence is produced on a schedule.

Cybersecurity program and policies

Part 500 expects a formal cybersecurity program supported by written policies and procedures. Policies should be specific enough to guide operations and broad enough to evolve with the

business.

Create a policy set that covers access control, data security, incident response, business continuity, and third-party risk. Keep policies aligned to actual tooling and processes.

- **Evidence to keep:** Cybersecurity policy set, Program charter, Annual policy review records

Governance, CISO responsibilities, and reporting

Governance is a central theme. A qualified security leader is expected to oversee the program and report on risk and control performance to leadership.

Define CISO or equivalent responsibilities, schedule leadership reporting, and track program metrics such as vulnerabilities, incidents, and control exceptions.

- **Evidence to keep:** CISO reports to leadership, Security metrics dashboards, Board or executive meeting minutes

Risk assessment and asset inventory

Risk assessment is the anchor that justifies your control decisions. Asset inventory makes the risk assessment credible because you cannot protect what you have not identified.

Maintain an inventory of systems, data flows, and third parties. Update the risk assessment on a defined cadence and after major changes.

- **Evidence to keep:** Asset inventory exports, Data flow diagrams, Risk assessment reports, Risk register updates

Identity, access control, and MFA

Part 500 expects strong access control. Multi-factor authentication is commonly required for remote access and privileged access, depending on your risk and environment.

Centralize identity, enforce MFA, and implement periodic access reviews for key systems. Treat privileged access as a separate control area with stronger monitoring.

- **Evidence to keep:** MFA configuration evidence, Access review sign-offs, Privileged access audit logs

Logging, monitoring, and incident response

Covered entities must be able to detect, respond to, and recover from cybersecurity events. Incident reporting expectations mean you need clear decision paths and documented timelines.

Centralize logs, define alerting, create incident runbooks, and run tabletop exercises. Confirm what triggers external reporting and who owns communications.

- **Evidence to keep:** Centralized logging configuration, Incident response plan, Tabletop exercise results, Incident tickets and post-incident reviews

Vulnerability management and security testing

Vulnerability management and testing prove that controls are not theoretical. The regulation expects routine testing such as penetration testing and vulnerability assessments.

Define scanning schedules, remediation targets, and exception handling. Commission penetration testing and track remediation to closure, including retesting where needed.

- **Evidence to keep:** Vulnerability scan reports, Penetration test reports, Remediation tracking tickets, Retest evidence

Third-party security policy and oversight

Third-party risk is a major focus for financial services. Part 500 expects a third-party security policy and oversight of vendors that can access systems or data.

Tier vendors, define minimum security requirements, review evidence such as SOC reports, and document exceptions with compensating controls.

- **Evidence to keep:** Third-party risk policy, Vendor inventory and tiering, Vendor review records, Contract security clauses

Business continuity and disaster recovery

Operational resilience is part of cybersecurity. Part 500 expects business continuity and disaster recovery planning, with testing to prove recovery works.

Define recovery objectives, document runbooks, test restores and failovers, and track corrective actions after tests.

- **Evidence to keep:** BCDR plan, Backup and restore test results, Failover test evidence, Post-test remediation records

Reporting and certification considerations

Part 500 includes reporting obligations for certain cybersecurity events. It also includes periodic certification or acknowledgment requirements for compliance status. These obligations are hard to

meet if incident response is informal or if evidence is scattered across systems.

Build a reporting playbook before you need it

- **Define what is reportable:** Document what types of events trigger internal escalation and external reporting.
- **Assign decision owners:** Identify who decides that an event meets reporting criteria and who communicates externally.
- **Practice timelines:** Run tabletop exercises that include reporting steps, not only technical containment.
- **Maintain contact lists:** Keep regulator and partner contact information current and accessible during an incident.

Common pitfalls in Part 500 programs

- **Policies that do not match reality:** If the policy says you review logs daily, you need proof that it happens.
- **Unowned vendor oversight:** Third-party security reviews fail when they are not assigned and scheduled.
- **Incomplete asset inventory:** If key systems are missing from inventory, risk assessment and control coverage becomes questionable.
- **Inconsistent MFA enforcement:** Exceptions should be documented and justified. Silent exceptions become findings.
- **Testing without remediation tracking:** Penetration tests and scans need closure tracking and retesting evidence.

Implementation methodology for NYDFS Part 500

Phase 1: Determine coverage and scope

Confirm whether you are a covered entity or whether Part 500 applies through an affiliate or contractual requirement. Identify the systems and data in scope and establish program ownership.

Phase 2: Build and document controls

Implement the control areas that Part 500 expects. Prioritize identity, logging, vulnerability management, and third-party risk because those drive many compliance findings. Document policies and procedures that reflect actual practice.

Phase 3: Operate and produce recurring evidence

Move into steady-state routines such as access reviews, scans, penetration tests, incident exercises, vendor reviews, and BCDR tests. Keep artifacts organized so reporting and certification tasks do not become emergency projects.

How Jacobian Engineering supports NYDFS programs

NYDFS Part 500 compliance requires both governance work and technical execution. Jacobian Engineering supports FinTech and financial services teams with practical implementation.

- **Program readiness assessment:** Gap analysis, scope definition, and evidence planning.
- **Control implementation:** Identity and access management, logging and monitoring, vulnerability management, and BCDR improvements.
- **Policy and procedure writing:** Right-sized policies that match the operating model and satisfy audit expectations.
- **Security testing:** Penetration testing and remediation verification to support testing requirements.
- **Continuous compliance:** Compliance calendars and evidence routines that stay healthy between reporting cycles.

Business benefits

When implemented well, Part 500 work improves operational maturity and reduces risk exposure.

- **Clear accountability:** Defined roles and reporting improve decision making.
- **Reduced incident impact:** Monitoring and incident response routines improve containment and recovery.
- **Stronger vendor posture:** Third-party oversight reduces concentration risk and partner friction.
- **Better resilience:** BCDR testing improves reliability for customer-facing services.

FAQs

Are we a covered entity under NYDFS Part 500?

Coverage depends on your licensing and regulatory status in New York. Many vendors are not directly covered but still need to meet Part 500 expectations through contracts with covered

entities. Confirm coverage with counsel and your partner requirements.

Does NYDFS Part 500 require MFA everywhere?

The regulation strongly emphasizes MFA, especially for remote and privileged access. The exact implementation depends on your risk assessment, but MFA is commonly treated as a baseline expectation.

What evidence is most commonly requested?

Auditors and partners often ask for risk assessment records, policies, vulnerability management evidence, penetration test reports, access reviews, incident response documentation, and vendor review records.

How often do we need to test BCDR?

Part 500 expects periodic testing. The frequency should align to the criticality of the service and the results of your risk assessment. Many teams test backups more frequently than full failover.

Can a SOC 2 report help with NYDFS compliance?

SOC 2 evidence can support some control areas, but Part 500 has specific governance and reporting expectations. Use SOC 2 as supporting evidence, not as a substitute.

Primary references

- NYDFS Cybersecurity Regulation resources: dfs.ny.gov