GLOBAL DIGITAL FORENSICS · NEW YORK COMPUTER FORENSICS

NYDFS Part 500 Evidence Preparation Guide

For CISOs, compliance officers and security teams at DFS regulated banks, insurers and financial services companies.

Edition 2026-11-03 · Part of the New York Audit Preparation Pack at newyorkcomputerforensics.com/resources/new-york-cybersecurity-audit-preparation/

Use this guide to assemble the records a DFS examiner, an internal auditor or the officers signing the April 15 submission will ask for under 23 NYCRR Part 500. Start with three decisions, because they shape everything else: the legal entity, the review period and any limited exemption under section 500.19. Each checklist row then names the record to gather and the next step, and the companion CSV gives your team a column for the owner, the evidence reference and open questions.

Part 500 deadlines and records

Requirement	Timing and rule	Record to keep
Penetration testing	At least annually, from inside and outside the system boundaries, by a qualified internal or external party. 500.5(a)(1)	Approved scope, tester qualifications and dated results
Vulnerability scans	Automated scans plus manual review of systems the scans miss, at the frequency the risk assessment sets and promptly after material system changes. 500.5(a)(2)	Scan coverage, findings, tickets and retest records
Risk assessment	Reviewed and updated at least annually and whenever a business or technology change materially changes cyber risk. 500.9(a)	Dated assessment, approval and change record
Access review	All user access privileges reviewed at least annually; access removed promptly after departures. 500.7(a)(4) and (6)	Review sign offs and termination records
Multifactor authentication	Required for any individual accessing any information system since November 1, 2025; entities with a limited exemption apply it to remote access, third party applications with nonpublic information and privileged accounts. 500.12	Enforcement settings, exception list and any compensating controls the CISO approved in writing
Response and recovery testing	Incident response and continuity plans tested, and restoration from backups tested, at least annually. 500.16(d)	Exercise records, participants, restore results and corrective actions
Cybersecurity incident notice	As promptly as possible and no later than 72 hours after determining that a cybersecurity incident occurred. 500.17(a)	Determination time, basis, submission and updates
Extortion payment	Notice within 24 hours of payment; written explanation of the reasons and alternatives within 30 days. 500.17(c)	Payment time, notices and the decision record

© 2026 Global Digital Forensics, Inc. All rights reserved.

Requirement	Timing and rule	Record to keep
Annual submission	By April 15 for the prior calendar year: a certification of material compliance or an acknowledgment of noncompliance, signed by the highest ranking executive and the CISO. Supporting records kept five years. 500.17(b)	Signed submission and the records behind it

Preparation checklist

Work through each row with the owner of the record. The companion CSV in this pack (nydfs-preparation-checklist.csv) carries the same rows with columns for status, owner, evidence reference and open questions.

ID	Topic	Record to gather	Next step	Source
DFS-01	Entity and exemptions	Record the legal entity, its DFS license or registration, the review period and any limited exemption claimed under section 500.19.	Settle applicability before any control is marked required or excluded.	23 NYCRR 500.1, 500.19
DFS-02	Risk assessment and control decisions	Gather the approved risk assessment, its method, the material risks and the dated decision for each risk.	Trace each material risk to a control or an accepted exception.	23 NYCRR 500.9; DFS risk assessment guidance, September 10, 2026
DFS-03	Asset inventory reconciliation	Compare the asset inventory with identity, endpoint, cloud and third party records.	List every difference before choosing a test sample.	23 NYCRR 500.13
DFS-04	Penetration testing	Gather the inside and outside test scope, the tester's qualifications, the written permission and the dated results.	Confirm the test ran within the last year and that open findings have owners.	23 NYCRR 500.5(a)(1)
DFS-05	Vulnerability management	Collect scan coverage, the manual review of systems the scans miss, findings, tickets and retest records.	Link each closed finding to evidence that the weakness was fixed.	23 NYCRR 500.5(a)(2), 500.5(c)
DFS-06	Access and MFA	Request the annual access review, the privileged account list, MFA enforcement settings and any written CISO approval of compensating controls.	Show what the records prove for the review period, alongside what the policy says.	23 NYCRR 500.7, 500.12
DFS-07	Audit trail and monitoring	Gather the log source inventory, retention settings and sample event records.	Record the periods and systems each log source covers for the review period.	23 NYCRR 500.6, 500.14
DFS-08	Response and recovery	Gather the incident response and continuity plans, exercise records, backup restoration tests and corrective actions.	Confirm each test happened in the last year and who approved the result.	23 NYCRR 500.16

© 2026 Global Digital Forensics, Inc. All rights reserved.

ID	Topic	Record to gather	Next step	Source
DFS-09	Governance and independent audit	Request board reporting, CISO reports and, for Class A companies, the independent audit plan and results.	Keep penetration testing separate from the independent audit a Class A company needs.	23 NYCRR 500.2(c), 500.4
DFS-10	Annual submission record	Index the records supporting the certification or acknowledgment and confirm the two signatories.	Keep the supporting records for five years.	23 NYCRR 500.17(b)

Sources

- 23 NYCRR Part 500, NYDFS Cybersecurity Regulation (Second Amendment, effective November 1, 2023; department reading copy). Sections 500.1 to 500.24, including testing, risk assessment, access, MFA, recovery testing, notices and the annual submission. Checked 2026-11-03. https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500
- NYDFS, Guidance on How to Conduct and Use Risk Assessments Required by the DFS Cybersecurity Regulation, September 10, 2026. Documenting risks, linking each risk to controls and updating the assessment after material change. Checked 2026-11-03. https://www.dfs.ny.gov/industry_guidance/industry_letters/il20260910-cyber-risk-assessment
- NYDFS Cybersecurity Resource Center. Covered entity resources, exemption filings and the portal for notices and the annual submission. Checked 2026-11-03. https://www.dfs.ny.gov/cybersecurity

Scope Your Assessment

The first call is a free consultation with a senior security lead. We review the systems, the review or audit you face and its timing, and recommend the assessment depth that answers it. Requests are handled in confidence.

Call (800) 868-8189, 24/7 · New York office (212) 561-5860

Email info@evestigate.com or request your consultation at newyorkcomputerforensics.com/contact.