Preparing for a NYS DFS Cybersecurity Audit

Organize the examination request, responsible staff and initial evidence pack before responding to a New York financial services review.

Edition 2026-11-03 · Online at newyorkcomputerforensics.com/guides/nydfs-audit-preparation/

Start by identifying the request you actually received. An internal audit, a customer assessment and a DFS examination may require different evidence and different decision makers. Confirm the legal entity, review period, applicable Part 500 requirements and response deadline. Settle applicability and exemptions before the technical team marks any requirement complete. This short guide helps organize that preparation; the full Technical Evidence Playbook provides the more detailed working method. [NYDFS Cybersecurity FAQs]

Appoint a coordinator and preserve the request record

Name one person to maintain the request list, evidence index and delivery versions. Identify the owners for identity, infrastructure, applications, security operations, vendors and business continuity. Retain the original request and later clarifications. A response coordinator can then explain where each item stands while the underlying evidence stays as collected.

Establish scope before collecting files

Record the entity's systems, shared services, significant providers and relevant data. Confirm which evidence must describe historical operation and which concerns current settings. Ask owners to identify known gaps early, and date each new screenshot as a record of current settings. Keep original exports, collection dates, filters and explanations together.

Assemble a focused first evidence pack

Begin with the applicable policies, current risk assessment, asset inventory, access and MFA records, vulnerability and penetration test records, incident response and recovery exercise evidence, relevant provider material and the prior annual submission's support. Section 500.12 has required MFA for every individual accessing any information system since November 1, 2025. Check that each document covers the correct entity, systems and period.

For each material assertion, identify an evidence reference and a named owner who can explain it. Use samples deliberately and state what each one covers. A representative access removal record shows how the process operated for that departure, and a sample drawn across the year shows its operation over the period.

Reconcile exceptions instead of concealing them

Create a short register of missing records, contradictory dates, uncovered systems and open remediation. Record the consequence, owner, proposed next step and review date. Distinguish an exception discovered during preparation from a conclusion about whether the entity materially complied.

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

Use current DFS guidance when reviewing the risk assessment. The September 2026 guidance explains the value of documented risks, control traceability and updates when circumstances change. Tailor any borrowed framework to the entity's environment and risks. [NYDFS risk assessment guidance]

Confirm reporting and signatory responsibilities

Part 500 contains separate annual submission and incident notice provisions. Identify the responsible people and their support records before a deadline approaches. A certification of material compliance and an acknowledgment of noncompliance are different submission paths. Keep the supporting account aligned with the period and applicable text of the regulation. [NYDFS Cybersecurity Regulation]

Prepare for a reviewer to follow the account

Use consistent system names and dates, readable evidence references and concise explanations. Separate original records from annotated copies. Ask each control owner to verify factual accuracy, and arrange the appropriate legal or compliance review. Retain the delivered version and record later corrections. The objective is a response the examiner can follow and check.

Plan the applicable timing and evidence record

Confirm covered entity status and any section 500.19 exemption first, then assign an owner to each row and preserve the actual trigger time.

Selected Part 500 preparation dates and clocks

Selected obligation	Timing and section	Record to prepare
Internal and external penetration tests	At least annually; §500.5(a)(1).	Approved scope, qualified tester and dated results.
Vulnerability scans and uncovered system review	Risk assessment frequency and promptly after material system changes; §500.5(a)(2).	Coverage, findings and closure evidence.
Risk assessment	Review at least annually and after a material change in cyber risk; §500.9.	Dated assessment and change rationale.
Defined cybersecurity incident notice	Promptly, no later than 72 hours after determination; §§500.1(g), 500.17(a).	Determination time, basis, submission and updates.
Annual submission	By April 15 for the prior calendar year; §500.17(b).	Certification of material compliance or acknowledgment of noncompliance, signed by the highest ranking executive and the CISO, with supporting records.
Extortion payment notices	Notice within 24 hours and explanation within 30 days of payment; §500.17(c).	Payment time, notices and authorized decision record.
Response and recovery exercises	At least annually where §500.16(d) applies.	Participants, restore results and corrective actions.

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

Apply the defined cybersecurity incident test in section 500.1 and record when the determination was made.

NYDFS Part 500 source and definitions

Information Gathering Q&A Checklist

Use this Q&A with the people who own the systems and the relevant legal or business decisions. Mark unknown or not applicable answers explicitly. Record an owner, a confirming source and the date.

Record who controls access to each source and how a secure handoff can be arranged, and keep completed copies with the matter records the company maintains.

What exact audit or examination request and review period did you receive?

Identify the coordinator, the control owners and the response date.

Answer:

Owner, source, date and open questions:

Which legal entity and license are covered, and does any exemption apply?

Record the entity, its DFS license or registration and any limited exemption claimed under section 500.19, with the person who made that decision. [NYDFS Cybersecurity Regulation]

Answer:

Owner, source, date and open questions:

Who coordinates the response, and who owns each control area?

Name the owners for identity, infrastructure, applications, security operations, vendors and recovery, and the person who keeps the request list.

Answer:

Owner, source, date and open questions:

Is the current risk assessment dated, approved and traceable to controls?

Collect the assessment, its approval, the last update and the record that links each material risk to a control or accepted exception. [NYDFS risk assessment guidance]

Answer:

Owner, source, date and open questions:

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

Can you show MFA for every individual who accesses your information systems?

Section 500.12 has required MFA for any individual accessing any information system since November 1, 2025. Gather the enforcement settings, the exception list and any compensating controls the CISO approved in writing. [NYDFS Cybersecurity Regulation]

Answer:

Owner, source, date and open questions:

Where are the latest penetration test and vulnerability scan results?

Gather the annual penetration test, the scan coverage, the findings and the remediation and retest records under section 500.5.

Answer:

Owner, source, date and open questions:

Which response and recovery exercises were held this year?

Collect the incident response and continuity exercise records and the backup restoration test required at least annually by section 500.16(d).

Answer:

Owner, source, date and open questions:

What supported the last April 15 submission, and who signed it?

Locate the certification or acknowledgment, the signatures of the highest ranking executive and the CISO and the records that support it under section 500.17(b).

Answer:

Owner, source, date and open questions:

Which open records or findings need an accountable next step?

Distinguish current remediation from evidence of past operation.

Answer:

Owner, source, date and open questions:

Primary sources and further reading

Sources checked November 3, 2026.

1. NYDFS Cybersecurity Regulation, 23 NYCRR Part 500 https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500

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

2. NYDFS risk assessment guidance, September 10, 2026 https://www.dfs.ny.gov/industry_guidance/industry_letters/il20260910-cyber-risk-assessment
3. NYDFS Cybersecurity FAQs https://www.dfs.ny.gov/cybersecurity/faqs

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.

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