The NYDFS 23 NYCRR Part 500 Technical Evidence Playbook

Connect Part 500 requirements with risk assessments, access records, testing results and the people responsible for each record.

Edition 2026-11-03 · Online at newyorkcomputerforensics.com/guides/nydfs-technical-evidence/

An examination response is easier to defend when the entity can connect a regulatory requirement to a named owner, the systems within scope, the control that operates there and evidence showing what happened during the relevant period. Operating records show that an account was removed, a backup restored or an incident evaluated on time, and each dashboard warning reads in its own scope and context.

This playbook helps a covered entity assemble and explain technical evidence for compliance leaders, the CISO, internal audit and authorized examiners. Determine the entity's obligations, exemptions and reporting requirements with the appropriate legal and compliance owners. Keep factual exceptions visible and distinguish current remediation from the state of controls during the period under review.

Establish the covered entity, examination period and applicable requirements

Begin with the legal entity and its relevant license, registration or other DFS authorization. Identify affiliates, shared services and providers that operate systems on its behalf. Record the examination period, the request or notice received and the person coordinating the response. Confirm whether a claimed exemption is current, documented and relevant to each requirement.

Use the official regulation and current DFS guidance to build the requirements register. Mark the basis for each applicability decision and preserve the approving person's record. Part 500 coverage follows the applicable rule and the entity's circumstances, and DFS obligations sit alongside any other regulator's oversight. [NYDFS Cybersecurity FAQs]

Create one evidence index with a clear chain to each assertion

Give each requirement or examination request a stable reference. For each response, identify the control owner, relevant systems, period, evidence source, collection date and location. Use a short explanation of what the evidence demonstrates. For example, a configuration export shows a setting at a point in time, while activity records may help demonstrate operation over a period.

Keep original exports separate from annotated presentation copies. Preserve the query, filters, source time zone, export options and errors. If the source is a provider portal, record the tenant and administrative scope used. Date each result generated today as current state, and draw the historical state from records of the period, keeping their timestamps and the earlier account intact.

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

Make the risk assessment traceable to actual business risk

Use the risk assessment to explain why particular assets, access routes and business processes matter. Connect identified risks to their control owners and supporting evidence. Keep the assessment's scope, assumptions, methodology, risk criteria and material exclusions with its findings.

DFS's September 2026 guidance emphasizes an assessment tailored to the entity, documented risks, traceability to controls and updates when circumstances change. Use that guidance alongside the regulation. Record management's remediation or risk acceptance decisions and the facts on which they relied. A later reassessment explains what changed and keeps the earlier result. [NYDFS risk assessment guidance]

Reconcile inventories with systems and data that actually exist

Compare the asset inventory with representative identity, endpoint, cloud, network and business application records. Identify owners, locations and significant dependencies. Include systems supplied through shared services and the information the entity needs from providers to understand them. Keep unmatched assets and undocumented owners as open items with an accountable next step.

An inventory supports an examination across its demonstrated coverage, so reconcile purchase records with virtual machines, tenant applications, provider infrastructure and offline or isolated systems. Document the collection methods and reconciliation process. The objective is an explainable inventory with its coverage stated.

Show how access is approved, reviewed and removed

Assemble evidence of account creation, privilege approval, periodic review and termination. Include ordinary users, privileged administrators, service identities, remote access and relevant provider access. Review a sample of actual personnel changes against the corresponding access records. Explain discrepancies with facts: a delayed disablement, an account used by a service or an approval that could not be located.

Since November 1, 2025, section 500.12 requires MFA for any individual accessing any information system of a covered entity, so the evidence covers every user population, including remote and privileged access. Distinguish the written policy, configured scope and effective enforcement. Preserve policy exports, exclusions, alternative control decisions where applicable and representative operating records. Identify the systems and people that the evidence actually covers. [NYDFS implementation timeline for covered entities]

Connect vulnerability findings to remediation and retesting

Keep the approved scope, asset coverage, assessment dates and material exclusions with penetration test and vulnerability assessment reports. Reconcile findings to responsible owners, remediation decisions, target dates and evidence of closure. Where a weakness was accepted or a fix deferred, retain the rationale and applicable compensating measures rather than quietly deleting the finding from a dashboard.

Show the distinction between an automated result, a validated weakness and a retest observation. A rescan can help determine whether a particular issue remains detectable under the retest conditions. It shows what the tested paths revealed during the tested period. If material systems were excluded, explain who authorized that boundary and what other evidence addresses the risk. Testing supports the entity's risk decisions and examination response.

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

Explain logging, monitoring and historical coverage

For important sources, record the enabled events, collection path, retention, time synchronization and responsible monitoring team. Identify whether records are provider generated, forwarded to another platform or stored locally. Preserve evidence that alerts were received and handled where the examination concerns monitoring operation.

Build a coverage table for the review period. Mark earliest and latest available records, known interruptions and relevant changes to settings or licenses. Where the entity relies on a provider, request the specific evidence needed and retain the provider's stated coverage and exceptions. Use a suitably scoped or redacted record wherever personal information appears.

Demonstrate recovery through actual exercise records

Collect the incident response and business continuity or disaster recovery plans applicable to the reviewed systems. Identify the people responsible for using them, the exercises performed and the resulting corrective actions. For restoration evidence, distinguish a backup job's reported completion from an observed recovery of the required data or system.

Preserve the exercise scenario, participants, start and finish times, dependencies, exceptions and decisions. If the exercise was limited to a sample or an isolated environment, say so. Record how open findings were assigned and followed through. A complete account records each restoration step, including any failure, its consequence and the remediation. [NYDFS Cybersecurity Regulation]

Address third parties and shared responsibility directly

List the providers relevant to each request and identify the business owner responsible for the relationship. Match the entity's claimed control to the contract, available assurance material and any direct operating evidence. Read the scope, period and exceptions in provider reports rather than treating the report's existence as confirmation of every service the entity uses.

Where responsibilities are divided, document who approves access, enables logging, preserves evidence and responds to an incident. A provider may operate infrastructure while the entity remains responsible for tenant settings or user access. Keep open requests visible, and where a provider's historical evidence runs short, identify alternative records. Read each assurance letter for the facts it addresses.

Preserve the incident and notification decision record

Maintain a chronology separating initial detection, escalation, determination, containment, evidence collection and notifications. Record who made the relevant determination, the facts known at that point and the time of each submission or update. Apply the regulatory analysis alongside any internal severity label.

Part 500 also contains distinct provisions for extortion payment notices and explanations. Keep payment related decisions under the direction of authorized leadership. Technical personnel should preserve the factual account and identify changing information promptly. [NYDFS Cybersecurity Regulation]

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

Support the annual submission with the record it actually requires

Identify the data and documentation supporting the entity's annual submission and the responsible signatories. Distinguish a current improvement project from evidence about the prior calendar year. The regulation provides different submission paths, including certification of material compliance and acknowledgment of noncompliance. The highest ranking executive and the CISO sign whichever path the record supports.

Keep the supporting records and known areas requiring improvement together with remediation plans and their status. Preserve versions and approvals so the entity can explain the account later. A technical specialist reconciles the evidence so the signatories sign on a record they understand. [NYDFS Cybersecurity Regulation]

Deliver a response package that a reviewer can follow

Prepare a concise response narrative and link it to the indexed supporting records. Use consistent entity names, system identifiers, dates and evidence references. Separate facts, interpretations and open questions. Identify documents supplied by a provider and statements resting on an interview. Make each source visible and keep the package focused on the request.

Before delivery, have the control owner confirm factual accuracy and have compliance review the response. Test whether a person unfamiliar with the project can follow a material assertion to its support. Resolve broken references, conflicting dates and unexplained gaps. Preserve the delivered version and the record of later corrections. That produces an examination response whose reasoning can be checked, even when the underlying environment still contains work to do.

Plan the applicable timing and evidence record

Settle covered entity status and any limited exemption before using the table. Each row needs an owner, and each clock runs from the actual trigger time, so record it when it happens.

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.

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

Selected obligation	Timing and section	Record to prepare
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.

The 72 hour clock starts when the entity determines that a cybersecurity incident as defined in section 500.1 occurred, so the evidence file should show who made that determination and when.

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.

Which covered entity, review period and examination requests are in scope?

Identify the applicability and exemption decision owner.

Answer:

Owner, source, date and open questions:

Where is the evidence index kept, and who maintains it?

Name the index, its owner and the rule for recording each delivered version.

Answer:

Owner, source, date and open questions:

Do the asset inventory, identity records and endpoint records reconcile?

Compare the inventory required by section 500.13 with directory, endpoint management and cloud records, and list every difference. [NYDFS Cybersecurity Regulation]

Answer:

Owner, source, date and open questions:

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

How is access approved, reviewed and removed, and where is the proof?

Gather the approval records, the annual access review and the departure records that show prompt termination under section 500.7.

Answer:

Owner, source, date and open questions:

Which log sources exist, how long are they kept and where are the gaps?

List each audit trail source, its retention setting and any period or system without coverage.

Answer:

Owner, source, date and open questions:

Which third party service providers hold nonpublic information?

Collect the provider list, the diligence performed and the contract terms required by section 500.11.

Answer:

Owner, source, date and open questions:

Which cybersecurity events were assessed during the period, and when was each decided?

Record the determination time, the basis and any notice to DFS, which section 500.17(a) requires within 72 hours of determining that a cybersecurity incident occurred.

Answer:

Owner, source, date and open questions:

Which control assertions lack current or historical supporting records?

Assign an owner, a source request and a response date for each one.

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
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

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

4. NYDFS implementation timeline for covered entities https://www.dfs.ny.gov/system/files/documents/2023/11/cybersecurity_implementation_timeline_covered_entities.pdf

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.