Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/nydfs-500-technical-evidence/

FINANCIAL SERVICES CONTROL EVIDENCE

Validating Shared NYDFS Part 500 Controls Across Affiliates and Third Parties

A Part 500 examiner looks for evidence that the covered entity's own systems were tested, inventoried and protected, beyond a parent company's assurance. Gather the testing, access and inventory records now and complete remediation before the April submission. Call (800) 868-8189 at any hour.

Published September 5, 2026 · Updated October 30, 2026

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

Why Part 500 Examiners Look for Entity Specific Technical Evidence

Financial institutions, insurance carriers, fintech operators and mortgage lenders regulated by the New York State Department of Financial Services face some of the strictest cybersecurity mandates in the nation under amended 23 NYCRR Part 500. When a regulated covered entity relies on shared IT infrastructure, Active Directory domains or Security Operations Center monitoring provided by a parent corporation or an affiliate, examiners look past a high level memo about the parent company to the entity's own records. Regulated entities produce concrete technical evidence that penetration testing, multi factor authentication, privileged access management and asset inventories actually cover the specific systems and attack paths serving the New York entity.

Generating Defensible Penetration Testing and Control Evidence for Annual Certification

Global Digital Forensics partners with Chief Information Security Officers, internal auditors and regulatory counsel to execute manual penetration testing and technical control validation tailored specifically to NYDFS Part 500 standards. Our engineers test both external perimeters and internal lateral movement paths across shared parent and affiliate network boundaries, verifying whether a compromise in an unregulated sister subsidiary can pivot into the covered financial entity environment. Every engagement concludes with a dual layered executive and technical report, complete with verification retesting records, giving your CISO and highest ranking executive, the two officers who sign the annual Part 500 submission, the evidentiary binder behind it.

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

Which Sections Demand Evidence and What the Text Requires

Section 500.5 is where most examinations start. It requires penetration testing of the covered entity's information systems from both inside and outside the information systems' boundaries by a qualified internal or external party at least annually, along with automated scans or manual reviews designed to find vulnerabilities at a frequency set by the risk assessment. The word inside is the one that deserves the most attention. The section calls for testing that continues past the perimeter into internal systems, and for a penetration test as a record distinct from a scan report. Section 500.7 limits user access privileges and, for Class A companies, requires privileged access management, while section 500.12, since November 1, 2025, requires multi factor authentication for any individual accessing any of the entity's information systems, with the narrower list of remote access and privileged accounts reserved for entities that qualify for the limited exemption in section 500.19(a). Each of those produces records an examiner can ask to see.

The remaining clocks are specific and we design engagements around them. Section 500.17 requires notice to the superintendent as promptly as possible but no later than 72 hours after determining that a cybersecurity incident occurred at the entity, an affiliate or a third party service provider, notice within 24 hours of any extortion payment with a written explanation of why payment was necessary within 30 days, and the annual compliance submission by April 15 covering the prior calendar year, signed by the highest ranking executive and the CISO. Section 500.13 requires an asset inventory with owner, location, classification, support expiration and recovery objectives for each asset, and section 500.16 requires incident response and business continuity plans that are tested. The NYDFS records preparation package maps each of these sections to the documents a CISO should be able to produce on request.

Two further sections shape the scope of everything else. Section 500.9 requires a periodic risk assessment that is updated as reasonably necessary and that informs the design of the cybersecurity program, and the Department's September 2026 industry letter, already cited on this page, makes clear that examiners expect the risk assessment to drive the frequency and depth of testing rather than the other way around. Section 500.11 requires written policies for third party service providers with access to the entity's systems or nonpublic information, including due diligence and periodic assessment of those providers' practices. A testing scope drawn from the risk assessment includes the vendor connections and shared services it identifies, which gives the entity a ready answer when the examiner asks how the scope was set.

What a Testing Record Establishes and How Examiners Read It

A defensible penetration testing record has layers. The scope letter and rules of engagement establish which systems were in bounds and why those systems are the covered entity's information systems rather than a sample. The tester's working notes, raw tool output and timestamped screenshots establish what was tried, from external reconnaissance through internal lateral movement toward the systems that hold nonpublic information. The findings report establishes what was found and its severity, and the retest record establishes what was fixed. Together they let an examiner trace a path from the regulation's words to the evidence directly. We deliver all of those layers because a complete set is built to answer the examiner's questions in the order they are asked.

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

Control evidence has the same structure. For multi factor authentication we collect conditional access policy exports, the list of accounts excluded from those policies and the sign in logs that show enforcement rather than configuration. For access privileges we collect the privileged role assignments, the periodic review records and, for Class A companies, the privileged access management session logs. For the asset inventory we reconcile the maintained list against what discovery actually finds on the network, because any difference between the two is itself a finding. We also state the reach of each record plainly. A penetration test is a point in time result, a conditional access export shows policy on the day it was taken, and a shared security operations center's coverage of the covered entity is read from its alert rules and asset scope.

Phases of a Part 500 Validation Engagement

Scoping begins with the covered entity's own definition of its information systems, then follows every dependency outward into the parent, the affiliates and the third party service providers that section 500.11 requires the entity to assess. We document that map because the examiner will ask how the boundary was drawn. Rules of engagement are agreed with the CISO and, where litigation or enforcement exposure exists, with regulatory counsel so that the work product is handled appropriately. The testing then runs from outside in: external attack surface and exposed services first, then authenticated internal testing from the position of a compromised workstation or an affiliate network, aimed at the systems that hold nonpublic information.

Control validation runs alongside the testing. We verify multi factor coverage by attempting authentication paths rather than reading policy, review privileged access against the account inventory, test whether the asset inventory matches the live environment and examine whether incident response plans have actually been exercised. Findings go to the CISO as they are confirmed so remediation can start before the report is final, and a retest window is built into the schedule so that critical findings are closed and retested before the certification date. The final deliverable is a two layer report, an executive narrative for the senior governing body and a technical appendix with the evidence, that functions as the binder behind the annual submission. Our penetration testing and vulnerability assessment pages describe the testing disciplines in more detail.

Where Covered Entities Gain Ground in an Examination

The first gain is ownership. An entity that answers a document request with its own testing and control records, alongside any parent company attestation or shared services memo, shows the examiner that it holds its own evidence. The second is scope. Penetration testing that runs inside and outside the boundary, recorded separately from the scans and covering the systems that hold nonpublic information, meets the section on its own terms. The third is timing. Testing completed early leaves room to remediate and retest, so the certification rests on closed findings rather than the open critical findings that appear in consent orders. The fourth is the Class A threshold: entities that cross it adopt the additional requirements for independent audits, privileged access management and endpoint detection ahead of the next examination.

Preparation starts well before the first call with us. The CISO assembles the current information systems inventory, the prior year's testing reports and remediation evidence, the risk assessment and the list of third party service providers with access. Internal audit identifies which findings from prior examinations or audits remain open. Regulatory counsel confirms whether any cybersecurity events during the year met the 500.17

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

notice thresholds and whether those notices were made. With those materials in hand, the scoping conversation goes straight to the open items. Entities also preparing for broader regulatory calendars will find our annual compliance testing guide and our financial services practice page useful companions.

Internal auditors and counsel read the resulting evidence differently, and the report serves both. The auditor traces each regulatory requirement to a tested control and a dated artifact, looking for the gaps between what the policy says, what the configuration shows and what the test demonstrated. Counsel reads for exposure: which findings, if left open, could support a Department allegation that the certification was inaccurate, and which cybersecurity events during the year met a notice threshold. The CISO reads for remediation priority. Writing one report that each of them can use directly is a deliberate choice, because an examination request moves quickly, and a binder that already speaks the regulation's language lets the entity answer at the same pace.

Scope Your Part 500 Assessment Before Your Certification Window

Start with our NYDFS records preparation package, then call Global Digital Forensics at (800) 868-8189 or (212) 561-5860 to schedule your NYDFS Part 500 testing engagement. The initial consultation is free.

Part 500 Sections, the Evidence and the Clock

The guide explains that an examiner asks for concrete technical evidence alongside any memo. This table maps the Part 500 sections that most often draw questions to the evidence a covered entity should be able to produce and the deadline each carries. Read it as the binder behind the annual certification. The clocks in the notice rows run from the determination that a cybersecurity incident occurred, and the submission clock is fixed to the calendar.

Key sections of 23 NYCRR Part 500, the evidence each demands and the deadline attached.

Section	Evidence to produce	Clock or cadence
500.5 penetration testing	Inside and outside test records with methodology and retest	At least annually
500.7 access privileges	Role assignments and reviews, PAM logs for Class A	Periodic review
500.9 risk assessment	A current assessment that drives testing scope	Updated as reasonably necessary
500.11 third party providers	Due diligence and periodic assessment of providers	Periodic
500.12 multi factor authentication	Conditional access exports and enforcement sign in logs	Continuous
500.13 asset inventory	Inventory with owner, location, classification and recovery objectives	Maintained
500.17 notice and submission	Event notice and the annual compliance submission	72 hours and April 15

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

How to Begin and What Happens on the First Call

Before the call, our Penetration Test Readiness: Scope, Schedule and Retest Before Audit sets out the items to secure in the order they expire. Bring the covered entity's information systems inventory or your best current list, last year's penetration testing and vulnerability assessment reports with remediation records, the current risk assessment, the list of affiliates and third party service providers with access to your systems and the date of your next submission. Our engineer asks how the covered entity's boundary is drawn against the parent and affiliates, which systems hold nonpublic information, whether you are a Class A company, what findings remain open and whether regulatory counsel is involved. You then receive a written scope that names the systems and boundaries to be tested, a schedule that leaves room for remediation and retesting before April 15 and a proposal for the report your senior governing body will rely on. The initial consultation is free, and the hotline at (800) 868-8189 is answered 24/7.

Technical References and Further Reading

Primary sources and provider documentation behind this guide: DFS's September 10, 2026 risk assessment guidance, DFS cybersecurity resource center, Read sections 500.5 and 500.6 in the current DFS text, section 500.7 and section 500.16.

Authorities cited in this guide: 23 NYCRR Part 500, Cybersecurity Requirements for Financial Services Companies. Supplies the penetration testing, access privilege, multi factor, asset inventory, notice and annual submission requirements discussed here, in the amended regulation text published by the Department of Financial Services. DFS industry letter on cybersecurity risk assessments, September 10, 2026. States the Department's expectations for how the risk assessment should drive the frequency and scope of testing and controls, as published on the Department's site. NIST Cybersecurity Framework. Provides the control organization many covered entities use to map Part 500 obligations to their broader security program, in the current Framework 2.0 publication.

FREQUENTLY ASKED

Questions Counsel and Security Leaders Ask About Financial Services Control Evidence

Does a vulnerability scan satisfy the Part 500 penetration testing requirement?

Section 500.5 names penetration testing and vulnerability assessment as separate obligations, so each has its own record. Penetration testing must be performed from both inside and outside the information systems' boundaries by a qualified party at least annually, and it involves a tester attempting to exploit weaknesses and reach the systems that hold nonpublic information. Automated scanning identifies candidate vulnerabilities at a frequency your risk assessment sets, and manual review extends what scanners find. A complete response to a penetration testing request pairs the scan report with the tester's own record.

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

Our parent company runs security for the whole group. Is that enough?

Shared infrastructure is permitted, but the covered entity remains responsible for showing that its own information systems meet the regulation. That means testing that covers the covered entity's systems and the paths into them from the shared environment, multi factor and access records specific to the accounts that reach nonpublic information, and an asset inventory the covered entity can produce itself. Part 500 also allows an affiliate's program to be adopted when it covers the covered entity's systems, and the entity holds the evidence that it does. We help entities build that evidence to stand alongside the attestation.

How far ahead of the April 15 submission should we schedule testing?

Far enough that testing, remediation and retesting all complete before the highest ranking executive and the CISO sign. The drivers are the size of the environment, the number of affiliate boundaries to test, how much remediation is likely and whether your internal engineering teams can move quickly on findings. Entities that test in the first half of the year tend to certify on schedule, with remediation and retesting complete, which keeps the certification decision straightforward.

What determines the cost of a Part 500 testing engagement?

The initial consultation is free. The proposal reflects the number of systems and network segments in scope, how many affiliate or parent boundaries must be tested, whether application testing is included, the depth of control validation required for multi factor, privileged access and the asset inventory, whether the entity is Class A, and the reporting the senior governing body and counsel need. Consolidating Part 500 testing with other framework obligations in one engagement usually lowers the total compared with separate vendor efforts.

What do we do if the test finds a critical vulnerability right before certification?

Fix it, retest it and document both. The regulation allows an entity that cannot certify full compliance to submit an acknowledgment that identifies the sections not fully complied with and describes the remediation timeline, and regulatory counsel should weigh that path against certifying. We provide findings as they are confirmed, ahead of the final report, so the remediation window opens as early as possible, and we schedule retesting so the evidence of closure can be in hand before the submission date.

Web Addresses for the Sources Cited

1. from both inside and outside the information systems' boundaries: https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500
2. DFS's September 10, 2026 risk assessment guidance: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20260910-cyber-risk-assessment
3. DFS cybersecurity resource center: https://www.dfs.ny.gov/cybersecurity
4. Read sections 500.5 and 500.6 in the current DFS text: https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500#page=8
5. section 500.7: https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500#page=9
6. section 500.16: https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500#page=14
7. NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

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

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

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