Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/audit-discovery-preparation/01-nydfs/

AUDIT AND DISCOVERY PREPARATION

New York DFS information gathering package

Gather entity facts, Part 500 cybersecurity records and open questions before a New York DFS review with your auditor or consultant.

Prepare an organized set of entity facts and existing cybersecurity records for a Part 500 auditor or consultant.

Business contacts, compliance teams, CISOs, project coordinators and internal IT

23 NYCRR Part 500 preparation for a potentially covered legal entity. Other DFS examination areas, such as financial condition, anti money laundering or transaction monitoring, call for their own preparation.

Before you gather

Start with the DFS license or other authorization and the legal entity's identity, because coverage turns on that document. Coverage under 500.1(e) follows the authorization itself, so presence in New York, handling New York data or supplying a regulated customer are recorded as context for the specialist alongside it. Ask counsel to document the basis for coverage and any exemption, and file that memorandum as the first record in the index; an examiner will ask for it before any policy.

A limited exemption under 500.19(a) removes specified duties, and the rest of the regulation continues to apply. Gather the underlying employee and independent contractor counts, the revenue, the assets and the affiliate information with their source reports, and let the specialist apply the exact definitions. Class A status also depends on specific revenue, employee and affiliate calculations, and the calculation itself is the evidence. Class A independent audits under 500.2(c), the annual filing under 500.17(b), a DFS examination and a consultant readiness review are four different activities; the Class A audit is based on the risk assessment, so describe it the way the regulation does, as an audit designed and conducted from that risk assessment.

Use the adopted amendment as the regulatory evidence and the clearly marked DFS reading copy for navigation. The September 10 2026 risk assessment letter is guidance. Ask the receiving professional to reconcile the current consolidated rule, the amendments and the examination request before fixing the final evidence list, because a package keyed to the section numbers in the examiner's request is the package the examiner can follow.

Give each request to the suggested owner. Record each answer, including the items awaiting confirmation, in the editable CSV checklist. Keep the records themselves in a secure evidence location agreed with the recipient and use the checklist as the index that points to them; passwords stay with their owners, and real

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

patient data and controlled technical information stay in the secure location.

Records to find

CSV files hold plain records, and your spreadsheet sets the layout. Import as UTF-8, keep IDs as text, wrap text and widen columns before use. Blank client fields are intentional.

DFS-R01 Entity and authorization file

Ask
Legal or compliance

Gather
Legal name, DFS license/registration numbers, authorizations, affiliate chart, covered activities and a copy of any examination letter.

Where to ask
Corporate records, licensing team, DFS correspondence

Why it may be needed
Lets the recipient identify the actual entity and engagement scope.

If missing or uncertain
Record which authorization or request the owner is tracing and who can obtain it.

Reference: DFS01 500.1(e); DFS04

DFS01 DFS04

DFS-R02 Exemption and Class A support

Ask
Finance, HR and compliance

Gather
Prior determinations and notices; employee/contractor counts and methods; relevant multi year revenue and year end assets; affiliates and shared systems/programs; changes to eligibility.

Where to ask
Finance reports, HR roster, corporate chart, submission receipts

Why it may be needed
Supports professional decisions under 500.1(d) and 500.19, which the specialist makes from the figures the coordinator gathers.

If missing or uncertain
Use Pending determination, and request the affiliate figures or dated receipt from finance or compliance.

Reference: DFS01 500.1(d), 500.19; DFS03

DFS01 DFS03

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

DFS-R03 Prior filings and regulator requests

Ask
Compliance

Gather
Prior calendar year certification or acknowledgment, supporting file, signatory authority, exemption notices, regulator correspondence and open examination items.

Where to ask
Compliance repository and DFS portal receipts

Why it may be needed
Connects the preparation period to actual submissions and requests.

If missing or uncertain
List the years, filing confirmations and signatory records to locate next. A certification rests on the supporting file and the signatory's own review, which the checklist feeds.

Reference: DFS01 500.17(b), 500.19; DFS03

DFS01 DFS03

DFS-R04 Program policies and approvals

Ask
CISO or security lead

Gather
Current and period relevant cybersecurity policies, operating procedures, approval records, policy revision history and any affiliate program adoption agreement.

Where to ask
Policy library, board portal, service agreements

Why it may be needed
Shows what the organization adopted and when; procedures and implementation records sit alongside the policy statements and are gathered with them.

If missing or uncertain
Supply draft or superseded documents with their status stated. Ask who holds the actual approval record.

Reference: DFS01 500.2, 500.3, 500.4; DFS04

DFS01 DFS04

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

DFS-R05 Governance and staffing records

Ask
Executive sponsor and HR

Gather
CISO appointment or service arrangement, responsible management, governing body reports, relevant minutes, budget/resource decisions and qualifications/training of security staff.

Where to ask
Board records, HR, vendor agreements

Why it may be needed
Helps the auditor plan interviews and understand responsibility and oversight.

If missing or uncertain
Provide names and dates, and sort each report as located, being traced or confirmed by its owner as never prepared.

Reference: DFS01 500.4, 500.10

DFS01

DFS-R06 Risk assessment history

Ask
Risk lead

Gather
Current and prior assessments, methodology, scoped systems/data, business inputs, threats, vulnerabilities, control evidence, accepted risks and resulting action plans.

Where to ask
Risk register and assessment repository

Why it may be needed
Shows why risks and controls were selected and whether changes were considered. The 2026 letter emphasizes traceable, business specific work.

If missing or uncertain
Log systems outside the assessment, rationale to trace and updates awaiting approval as questions for the specialist.

Reference: DFS01 500.9; DFS05

DFS01 DFS05

DFS-R07 System and data inventory

Ask
IT and business system owners

Gather
Hardware/software/cloud/OT inventory where relevant, owners, locations, sensitivity, support dates, recovery objectives, network/data flow diagrams and inventory reconciliation records.

Where to ask
Asset register, network team, procurement and provider portals

Why it may be needed
Supports the scope of the review, including specialized systems and third party dependencies.

If missing or uncertain
Use the source atlas to identify candidate repositories for their owners to confirm.

Reference: DFS01 500.1(i), 500.13

DFS01

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

DFS-R08 Access and authentication records

Ask
Identity administrator

Gather
Account and privileged account lists, review/approval records, joiner/leaver examples, MFA configurations and coverage/exclusions, remote access settings and written compensating control approvals.

Where to ask
Identity, HR, application administrators and provider

Why it may be needed
Allows the specialist to compare approved access with actual covered systems.

If missing or uncertain
Describe the systems outside the standard configuration and the review periods to trace with the owner.

Reference: DFS01 500.7, 500.12

DFS01

DFS-R09 Existing vulnerability and penetration test records

Ask
Security lead and service provider

Gather
Scope, qualifications, dated internal/external penetration test reports, scan/manual review coverage, risk based schedule, significant change records, remediation tickets and existing retest results.

Where to ask
Security provider and ticket system

Why it may be needed
Prepares the 500.5 review. Obtain existing work first; scanners, penetration testing and an audit are different activities.

If missing or uncertain
Record which scope or results the provider is tracing and request professional planning. Any new test starts with written authorization, safe scope and third party permissions.

Reference: DFS01 500.5; NI05

DFS01 NI05

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

DFS-R10 Logs and reconstruction examples

Ask
Security operations and finance systems

Gather
Logging policy, inventory, actual earliest/latest retained dates, protected storage, alert review records, and examples of reconstructing a material financial transaction and a relevant cyber event.

Where to ask
SIEM, financial application owner, archive and provider

Why it may be needed
500.6 distinguishes transaction records from cyber audit trails. The examiner confirms actual coverage from the retained dates themselves, with the product retention setting as the starting point.

If missing or uncertain
Identify the systems and time periods to confirm, and whether the source was configured to log the activity.

Reference: DFS02 500.6; DFS01 500.14

DFS02 DFS01

DFS-R11 Application and supplier records

Ask
Application owners and procurement

Gather
Application security procedures/reviews, change records, third party inventory, risk based due diligence, security clauses, incident notice terms and reassessments.

Where to ask
Development, procurement, vendor management and contracts

Why it may be needed
Connects internal and external services to the entity scope and evidence responsibilities.

If missing or uncertain
Request the actual contract and shared responsibility records to accompany any vendor certificate.

Reference: DFS01 500.8, 500.11

DFS01

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

DFS-R12 Encryption and disposal records

Ask
IT and records management

Gather
Data inventory, encryption coverage/key management descriptions, exceptions and approvals, disposal policy, retention schedule and disposal records with preservation overrides.

Where to ask
Storage, application owners, records team

Why it may be needed
Lets the specialist trace protection and lifecycle decisions to the relevant information.

If missing or uncertain
Describe open questions about keys, backups or disposal in plain terms, and keep secrets with their owners. Ask counsel about retention conflicts.

Reference: DFS01 500.13, 500.15

DFS01

DFS-R13 Monitoring and training records

Ask
Security operations and HR

Gather
Risk based monitoring coverage, detection and filtering descriptions, training content/attendance and social engineering exercises if conducted; Class A EDR/centralized logging records if potentially relevant.

Where to ask
SOC, learning platform and providers

Why it may be needed
Supplies actual operational records for monitoring/training and conditional Class A review.

If missing or uncertain
List the dates to locate and the personnel or systems outside the program; the specialist determines relevance.

Reference: DFS01 500.14

DFS01

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

DFS-R14 Response and recovery records

Ask
Continuity lead and IT

Gather
Incident response and business continuity/disaster recovery plans; staff roles/training; offsite backup scope/protection; existing annual exercises and critical data/system restoration results; after action updates.

Where to ask
Continuity system, backup team, providers

Why it may be needed
Supports review of prepared plans, staff participation and actual restoration evidence.

If missing or uncertain
Document an untested dependency as a question. Restoration is evidenced by a recorded restore exercise, so gather those records alongside the backup job reports.

Reference: DFS01 500.16

DFS01

DFS-R15 Incident and notice chronology

Ask
Legal and incident lead

Gather
Incident inventory, determination times, decision records, third party notices, DFS submissions/updates and extortion payment records if any, kept in a restricted workspace.

Where to ask
Incident case files, legal and compliance

Why it may be needed
Specialists need facts to evaluate distinct incident, payment and other reporting clocks.

If missing or uncertain
Escalate an active incident immediately. Record each time awaiting confirmation as an open item.

Reference: DFS01 500.1(g), 500.17; DFS03

DFS01 DFS03

DFS-R16 Prior assurance and open actions

Ask
Internal audit and project lead

Gather
Prior independent audit reports if applicable, scope and independence records, management responses, open actions, assigned owners, target dates and existing verification records.

Where to ask
Audit/risk repository

Why it may be needed
Lets the recipient see earlier work, its scope and the open matters, each with its current status.

If missing or uncertain
Track evidence being traced, proposed corrective actions and accepted verification as three separate entries.

Reference: DFS01 500.2(c), 500.17(b)

DFS01

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

Questions for client IT and owners

A useful answer names the actual system, period, supporting record and its coverage. Where the answer sits with someone else, name the person or provider who can give it.

1. Which legal entity and DFS authorization does the request concern?

Suggested responder
Legal or compliance

Useful supporting record
Attach authorization and examination request or record who has them.

2. Which period, systems and affiliates does the receiving professional expect to review?

Suggested responder
Engagement sponsor and auditor

Useful supporting record
Return a marked diagram and entity list.

3. Which MFA routes, privileged accounts and older applications are outside the normal configuration?

Suggested responder
Identity and application owners

Useful supporting record
Provide dated coverage and exception records; credentials stay with their owners.

4. What did the last internal and external penetration tests actually cover?

Suggested responder
Security lead

Useful supporting record
Return scope, dates, reports and exclusions.

5. How did the risk assessment affect decisions about each critical service and common provider?

Suggested responder
Risk and service owners

Useful supporting record
Link risk entries, decisions, control records and action owners.

6. Which logs are retrievable for the review period?

Suggested responder
Security operations

Useful supporting record
List each source, earliest/latest dates, gaps and relevant retention policy.

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

7. What evidence shows a critical system was restored and used successfully?

Suggested responder
Recovery owner

Useful supporting record
Supply actual exercise records with their stated scope.

8. Who can securely supply the remaining records and approve disclosure to the recipient?

Suggested responder
Project sponsor

Useful supporting record
Provide a responsibility list and approved transfer route.

Facts to confirm and specialist decisions

These are explicit handoff questions, and each one closes with the specialist's written answer, drawing on the records marked Received. Add client specific questions and a responsible person.

DFS-Q01 Does this legal entity qualify as covered, exempt or Class A for the period?

Ask
Counsel and receiving Part 500 specialist

Gather
Authorizations, affiliate facts, figures and prior notices

Resolution needed
Written period specific scope determination by counsel and the specialist, made from the gathered records.

DFS-Q02 Is the planned engagement a DFS examination, Class A independent audit, internal review or readiness consultation?

Ask
Sponsor and receiving auditor

Gather
Examination letter, charter and intended deliverables

Resolution needed
Agreed scope, independence, criteria and recipient responsibilities.

Preparing the handoff

The handoff is ready when the engagement sponsor has confirmed the entity and the period, with exemption and Class A issues marked pending where they are open; when each applicable preparation request has a response or a named follow up with its period and next owner; when restricted incident and testing material is indexed and delivered through the agreed secure route rather than an ordinary email attachment; and when the specialist has received the actual examination request and can determine the final criteria and evidence sufficiency from it.

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

Sources for this package

Official laws/rules establish duties within their scope. Guidance explains programs; NIST supplies methods; vendor documentation describes possible product behavior. The package works alongside the actual contracts, facts, configuration and case orders.

- DFS final adopted second amendment to Part 500 (DFS01)
- DFS Part 500 reading copy (DFS02)
- DFS cybersecurity submissions (DFS03)
- DFS cybersecurity FAQs (DFS04)
- DFS risk assessment guidance September 10 2026 (DFS05)
- DFS regulatory activity (DFS06)
- NIST SP 800-115 (NI05)

Bring the completed pack to a free scoping call and a senior examiner sets the scope from it. Call (800) 868-8189.

Source review date: October 18 2026.

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

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.