Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/ny-utility-audit-manual/

NEW YORK UTILITY CYBERSECURITY AND PRIVACY AUDIT MANUAL

The New York Utility Audit Manual Starts by Settling the Boundary

A New York utility audit starts from a settled boundary: the legal entity, the systems and the review period, each decided and recorded before the first evidence request. This manual maps PSC Part 1200, DFS Part 500 and private information duties to examination procedures, keeps safe field methods separate from compliance criteria and lists the authority questions to settle with counsel.

Start by choosing the audit boundary

Everything that follows depends on one decision: which entity, which systems and which period the audit covers. The Public Service Commission's Part 1200, the Department of Financial Services' Part 500 and New York's breach and safeguards laws each draw that boundary differently, and a utility that lets an auditor assume the answer inherits the dispute later. Settle the boundary first and record the reasoning, and the rest of this manual becomes a sequence of controlled records rather than a scramble.

First decisions

Identify each legal entity, the services it performs, its customers and employees, the systems under review and the review period, and write them on one page with the source for each fact. A holding company, a utility operating company, a licensed insurance affiliate and an operating contractor can have different obligations while sharing the same billing system and the same identity directory, and the shared system is where the boundary dispute will surface. The artifact is an entity to system map with a column for each regime, and it is the first document an auditor asks for.

Use the records in sequence

Complete Applicability before treating any control as a legal requirement. Use Work plan to allocate people, dates and dependencies. Record Data flows, select Control tests and retain controlled Evidence references. Use Findings and Notices for decisions, then Recurring duties and Handover for continuing ownership. Starting in Applicability ties every result in Control tests to a criterion, and that link is what the audit lead reads first.

Written approval for field work

Access to a utility system, collection of private information and live testing each proceed on the written approval of a named person.

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

What This Manual Establishes

The pack maps selected New York utility IT, customer privacy and DFS requirements to proposed examination work. Entity specific orders, local policies, confidential regulator directions, current tariffs and actual system evidence complete the audit basis, and the New York utility audit questions for counsel list what to settle first.

When the holding company, the operating company and the affiliate draw the boundary differently, put the question to a senior examiner before the audit period opens.

Sources: P01 Adoption of utility IT cybersecurity regulations, D01 Cybersecurity Regulation Part 500, B01 Private information breach notification, B02 Reasonable security safeguards, B03 State and local breach notification duties

---

Applying the Updated Audit Workbook

The workbook works as an execution record rather than a checklist. Every procedure row carries the fields an auditor reads first, and each row keeps an evidence gap and a supported conclusion in their own fields, so the reader sees at once which is which.

Pre Execution Readiness Checklist

Use all applicable procedures in the 41 row Control tests register. Freeze the exact criterion, the population, the review period, the sample rationale and the permitted method before anyone touches a system. Record the actual execution dates, the observations, the evidence identifiers and the reviewer when the work is done. A proposed procedure and a mapped clause prepare the assessment, and operating permissions are recorded in their own column beside the compliance criteria.

Pending Scope and Governance Decisions

The open count gathers every blank decision, every invalid decision text and every resolved selection awaiting a required record field. Fields present is the prompt for qualified review, and that review is what completes the row. The responsible people sign the approval fields once they have reviewed the work, and their signatures beside a zero open count are the record that the review took place.

Engagement Scope and Authorization

Record every proposed exclusion, its reason and the proposed responsible reviewer in Scope decisions. The builder preserves deferred task and test identifiers and the full 469 record PSC and DFS clause and context matrix. Examine the exact source text, the entity scope, the period, the decision evidence and the mapped test before recording an actual conclusion. Definitions, administrative provisions and appendix forms carry distinct labels, so each definition is read as context and each duty is tested as a duty. The operative DFS version, the utility specific criteria and questions Q01 to Q10 are resolved next, with counsel and written regulator direction.

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

Source Access and Revision History

The Sources sheet lists each source with the date it was reviewed. Request the current text of each source as you come to it, and keep its duty on the register while the text is on its way. Use the Edition record to track your own revisions and reviews, and keep the previous version when you adopt a new one.

The audit preparation walkthrough explains how to carry these execution records from the workbook into the scoping conversation.

Sources: N01 Assessing Security and Privacy Controls, N03 Guide to Operational Technology Security

---

Executive decisions and audit outputs

The sponsor's decisions define what the audit can conclude, and they are recorded before the first evidence request so the report can show that the scope was chosen rather than inherited.

Sponsor decisions

Approve the legal entities, the audit period, the business processes, the reporting audience, the budget and the access authority. Name the CISO, the privacy and data owners, the counsel or compliance decision maker, the operating authority, the project manager and the qualified audit lead, each with an alternate. Approve an escalation route for urgent exposure, unsafe work and potential regulatory notices, and test that route once before the audit period opens.

Required work products

The final project record includes a signed applicability matrix, approved scope and method permits, population and sample schedules, an evidence index, criterion level results, findings, corrective action decisions, retest results, notification decisions and a recurring duty calendar. The executive report identifies the material service and privacy risks, the scope questions awaiting a decision and the decisions that require resources. An auditor reviewing the engagement later will look for each of these by name.

Questions the report must answer

Which entity and period does each conclusion cover? Which controls were observed, tested, described by staff or not examined? What could interrupt billing, customer assistance, dispatch or restoration? What personal data could be exposed? Which actions have a mandatory deadline, who owns them, and what evidence supports closure? A report that answers the second question for every control keeps what staff said apart from what the auditor saw, and that separation gives each conclusion its weight.

Risk decisions

Use the utility approved risk criteria. Record the likelihood rationale, the consequence, the existing controls, the uncertainty and the residual exposure. A sponsor may prioritize investment or accept a residual business risk within authority. That entry sits alongside the duties set by law, rule, order, permit and contract, which continue to apply, and the record says so beside the signature.

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

Sources: N01 Assessing Security and Privacy Controls, D05 Risk assessment guidance

---

Applicability to DFS and shared services

Coverage under Part 500 is decided entity by entity from the authorization each one holds, and the artifact is the license or required authorization analysis for that entity.

Direct DFS coverage

Part 500 covers persons operating under or required to operate under qualifying Banking Law, Insurance Law or Financial Services Law authorizations. Retrieve the actual license or the required authorization analysis, the legal name and the regulator record, and file them with the applicability row.

Class A is a separate test

After coverage is established, test at least $20 million gross annual revenue in each of the last two fiscal years from all covered entity business operations and affiliates' New York operations, plus either more than 2,000 employees averaged over the last two fiscal years or more than $1 billion gross annual revenue in each of those years, using the specified worldwide group measures. Include only affiliates sharing information systems, cybersecurity resources or a cybersecurity program for this definition. Retain the calculation, the exact period and the source figures, because the calculation is the evidence.

Partial exemptions

Section 500.19(a) uses alternative employee or contractor, revenue or asset tests, with distinct affiliate and period rules. Read the full section and record which test each entity meets. An entity exempt from some provisions keeps its retained obligations, such as the applicable risk assessment, access controls, MFA, inventory, training and notices. File the required exemption notice, keep the filing receipt and monitor the triggers that would end the exemption.

Utility affiliate examples

A utility group with a separately DFS licensed captive or other licensed affiliate records its decision entity by entity. Adopting the parent's program retains covered entity responsibility and DFS evidence access. A utility acting only as a supplier takes its security duties from the contract, since covered entity status comes from the authorization an entity holds, and the contract is the record to read.

Sources: D01 Cybersecurity Regulation Part 500, D02 Cybersecurity resource center, D03 Requirements by exemption and entity category, D07 Adopting an affiliate cybersecurity program

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

Applicability of PSC Part 1200

Use the final adopted definition in section 1200.1(c), whose service connection and service line counts are more precise than the rounded 50,000 customer figure in press summaries.

Test	Decision evidence and boundary
Starting scope	A public utility company under PSL 2(23). Establish legal entity and jurisdiction before applying exclusions.
Water exclusion	Water works corporation serving fewer than 50,001 service connections under 16 NYCRR 501.1(c). A system with 50,000 such connections falls within the exclusion.
Electric exclusion	Electric corporation maintaining fewer than 50,000 service lines under 16 NYCRR 98.1(b). An electric corporation with 50,000 or more such lines is within the definition.
Gas exclusion	Gas corporation that is a SAPA 102(8) small business: resident in NY, independently owned and operated and 100 or fewer employees.
Other exclusions	Telephone corporations, solely telegraph operators and municipal corporations under GML 119-n are excluded by the definition. The agent/employee/designee exclusion has an express program coverage condition.
Public authority and mixed services	Verify charter, PSL classification, current orders and each actual function. Steam service is assessed under the general definition, with the size exclusions above written for water, electric and gas.

Sources: P01 Adoption of utility IT cybersecurity regulations, P08 Public utility definitions, P09 Small business definition

Applicability to personal information and ownership

The breach and safeguards duties follow the data and the entity's legal character rather than its office address, so the applicability row records who owns, licenses or merely maintains each class of information and where its subjects live.

Business safeguards and breach law

GBL 899-bb applies to a person or business owning or licensing computerized New York resident private information. GBL 899-aa defines private information and specifies breach duties for owners or licensees and for maintainers. Record where the data subjects reside, who owns or licenses the data and who merely maintains it, and keep the three roles separate on the data flow record. Residence of the data subjects and the role each party holds complete the test alongside any New York office location.

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

State entities

STL 208 defines state entities, including qualifying public authorities and public benefit corporations, with explicit exclusions for local agencies and the judiciary. Apply the entity's charter and its actual governmental function. Its private information definition, notice wording, ITS consultation and recipient rules get their own analysis, kept on its own checklist beside the GBL analysis.

Municipal and local operators

Cities, counties, municipalities, villages, towns and other local agencies are excluded from the state entity definition in STL 208(1)(c). Subdivision 10 separately requires them to adopt a notification policy or a consistent local law. Retrieve that actual instrument and file it, because it is the document that governs the local route. Resolve the GBL interaction, the operator contracts and the records requirements for the local route, and apply the state entity process where the charter and function call for it.

Smaller operators

SHIELD small business criteria are alternative tests: fewer than 50 employees; less than $3 million gross revenue in each of the last three fiscal years; or less than $5 million year end GAAP assets. SHIELD, existing PSC orders and contract duties each keep their own applicability test, so an entity within a Part 1200 size exclusion records a separate row for each regime.

Sources: B01 Private information breach notification, B02 Reasonable security safeguards, B03 State and local breach notification duties, P01 Adoption of utility IT cybersecurity regulations

---

Data definitions, classified before testing

Category	How the audit should treat it
PII	Use a broad inventory concept for linkable individuals, customer account data, workforce and contractor information. Breach notification is determined under the statutory definitions below, with PII serving as the inventory.
GBL private information	Apply 899-aa(1) combinations and conditions, including credentials permitting online account access and current medical and health insurance categories. Assess encryption and whether keys were compromised.
STL private information	Use 208(1) itself. Its displayed categories and breach definition are read on their own terms and compared with the current GBL wording. Document any interpretation issue.
PSC NPI	1200.1(j) includes specified business impact information, personal data, financial/billing records, health related data and identifiable consumption or use data.
DFS NPI	500.1(k) has its own business impact and individual/health information categories.
Energy usage	PSL 66(32) makes customer gas/electric consumption confidential. Analyze purpose, consent, tariff and data access orders for all such data, including usage data outside the GBL private information conditions.

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

Sources: B01 Private information breach notification, B03 State and local breach notification duties, P01 Adoption of utility IT cybersecurity regulations, D01 Cybersecurity Regulation Part 500, P07 Public Service Law section 66, N02 Protecting PII confidentiality

---

The 2013 PII order and current audits

The 2013 order still shapes what a large utility's annual audit looks like, and the transition to Part 1200 is decided clause by clause, with the legacy plan as the starting map.

Historical order

Case 13-M-0178 directed large electric, gas and water utilities to create implementation plans within 60 days of the August 19 2013 order. The order identifies nine recommendations and required a response explaining actions or reasons against implementation. The original 60 day deadline is historical and fixed to the 2013 order; the artifact to retrieve is the utility's own implementation plan and its audit history.

Nine recommendations

Plan breach response and recovery drills; retain qualified forensic response; arrange credit monitoring; strengthen employee and contractor privacy training; inventory and dispose of unnecessary customer information; segregate and mask sensitive information; improve physical protection; strengthen intrusion detection and security event management; and conduct regular third party vulnerability assessments. Each recommendation maps to a control test in this manual, and the mapping is recorded rather than assumed.

Annual external review

Pages 7 and 8 of the order describe annual third party audits and eight minimum examination areas. The first audit was to complete by July 1 2014, with subsequent annual audits commencing no later than the previous audit's one year completion anniversary. Retrieve the utility plan, the audit history and the current staff instructions, and set the audit period from the anniversary date in the file, which is the one that governs.

Relationship to Part 1200

The new rule says conflicting existing orders will be abrogated for covered companies as the regulations phase in, while existing orders continue for smaller noncovered companies. Build a clause level transition map. Part 1200.18 adds supply chain risk, IT and OT segmentation capability and compliance with the Part to its eleven area yearly third party audit.

Sources: P03 PII implementation plan order, P01 Adoption of utility IT cybersecurity regulations

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

Part 1200 transition and recurring calendar

Sources current to November 3, 2026. Record the operative interval and verify any computed calendar date, weekend treatment, written extensions and entity specific instructions.

Timing	Duty or planning action
June 1 2026	Effective date. Section 1200.21 applies from this date. Maintain incident/event logging and incident notice readiness from this date. First certificate expressly starts June 30 2027.
180 days from effective date	General transition for requirements not specially extended. Arithmetic reference: November 28 2026. Confirm the business day adjusted filing date with the regulator.
One year from effective date	1200.4(b),.5,.9,.11,.12,.14(b): CISO report, monitoring/testing, risk assessment, supplier/affiliate policy, access controls and awareness training.
18 months from effective date	1200.6,.8,.13,.14(a),.15: audit trails, application security, retention, user monitoring and encryption.
September 15 yearly	Third party audit made available to the designated DPS director under 1200.18(c). Resolve 2026 first year timing against the general transition and legacy annual duty; See the timing questions for counsel.
June 30 yearly from 2027	Prior calendar year compliance statement. Support retained five years. Confirm phased duty representation before signing; See the timing questions for counsel.

Sources: P01 Adoption of utility IT cybersecurity regulations, P02 Notice of adoption of Part 1200

Recurring duties after transition

Interval or trigger	Part 1200 requirement to assign
Yearly	CISO written report 1200.4(b); access review 1200.7(a); training 1200.14(b); encryption compensating control review 1200.15(b); response exercise 1200.16(c); qualified third party audit 1200.18.
At least every two years	Application security procedures 1200.8(b); risk assessment 1200.9, with change updates as reasonably necessary; provider/affiliate policy reassessment 1200.11(b).
Conditional testing	Absent effective continuous monitoring or other qualifying ongoing detection, penetration testing every 12 months and vulnerability assessments every 6 months under 1200.5. Verify the relied on alternative.
Within 90 days of exercise	Update incident plan based on yearly exercise results 1200.16(c). Record exercise date separately from update approval date.

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

Interval or trigger	Part 1200 requirement to assign
Within 10 calendar days of request	Specified program, policy, testing, risk, response, audit access, investigation report, log and certificate support records. Map exact requesting official and applicable clause.
Minimum retention	1200.6 audit trails at least 3 years; 1200.21(b) event/incident log at least 3 calendar years; 1200.21(c) certificate support 5 years. Other holds and record class duties remain.

Sources: P01 Adoption of utility IT cybersecurity regulations

---

DFS audit timing and filing differences

DFS duties run on their own calendar, so the PSC and DFS cycles each get their own set of dates and their own filing.

Recurring review

Subject to the actual exemptions, policies have annual approval, the risk assessment is reviewed and updated at least annually and upon a material risk changing business or technology change, access privileges receive at least an annual review, application security procedures receive an annual CISO or designee review, and training includes annual social engineering awareness. Inventory update and validation frequency follows the written procedures. Class A independent audits take their frequency from the risk assessment, set separately from the PSC calendar.

Testing and resilience

Current 500.5 requires at least annual internal and external penetration testing plus risk based scans and manual review of unscanned systems, with prompt assessment after material system changes. Current 500.16 calls for at least annual response and BCDR tests and critical data and system restoration testing. Apply partial exemptions clause by clause, and approve any OT method separately with the operating owner before a tester proposes it.

Annual filing

By April 15 submit either a certification of material compliance for the prior calendar year or the specified acknowledgment of noncompliance with the affected sections and a remediation timeline. The required signers are the highest ranking executive and the CISO, or the highest ranking executive and the responsible senior officer if there is no CISO. Retain the support for 5 years.

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

Amendment status

The 2023 second amendment's final two year transition for MFA and inventory ended November 1 2025. New status, exemption changes and specific instructions each receive an entity review, recorded with the version of the regulation it used.

Sources: D01 Cybersecurity Regulation Part 500, D03 Requirements by exemption and entity category, D04 Cybersecurity frequently asked questions, D05 Risk assessment guidance

---

Plan the project and establish authority

The project runs through four gates, and each gate has exit evidence that the project manager files before the next one opens.

Gate 1, scope

The project manager obtains the named entity, systems, period, sponsor, audit lead, data owners and operating owners. The compliance owner resolves each applicability row or names the evidence it awaits and the decision deadline. The audit lead confirms qualifications, independence where required, conflicts and access rights, and the confirmation is a signed record.

Gate 2, readiness

Build the evidence request list, the controlled exchange route, the stakeholder schedule, the population and sample plan and the method authorization. Confirm site induction, escort, collection devices, no photography areas, prohibited commands, incident escalation and data minimization rules. Scope expansion goes to the relevant authority for approval, and every request and its answer are logged.

Gate 3, examination

Collect existing configurations and records, interview owners, perform supervised demonstrations and permitted tests. Keep a daily discrepancy log, because the differences between the drawing and the system are the most useful record the examination produces. Report urgent vulnerabilities and possible incidents immediately through the approved process. The tester pauses and hands control to the operating authority on abnormal operation, a wrong target, lost visibility or unexpected private data exposure.

Gate 4, decision and closure

The audit lead reconciles findings to criterion and evidence. The sponsor funds and prioritizes action; counsel and compliance resolve legal interpretation and notices; the operating owner approves system changes. An independent or separately qualified retest records what changed and the result. The project manager hands over the remaining actions and the recurring duties. Proposed duration is set from the access, scope and testing plan agreed for the engagement.

Sources: N01 Assessing Security and Privacy Controls, N03 Guide to Operational Technology Security

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

Responsibilities and acceptance gates

Role	Accountability and acceptance evidence
Sponsor / governing body	Approves scope, resources and business risk decisions. Receives material issues and signs statements that are legally appropriate and backed by actual support.
CISO / technical lead	Owns program evidence, risk/control linkage, qualified testing and permitted exceptions. Technical approval states boundary, methods and any conditions awaiting a decision.
Compliance / legal / privacy	Owns instrument versions, entity specific applicability, information classification, disclosure basis, reporting clocks and regulator clarification.
Project manager	Maintains dependencies, people, due dates, requests, approvals, change log and handover. Tracks deadlines, while compliance and counsel make the legal compliance call.
Operating owner / technician	Operating owner controls live access, isolation and restoration authority. Technician follows approved runbook, logs observations and stops on defined conditions.
Auditor / reviewer	Defines tests, populations and evidence sufficiency. Tests each claim against evidence, reports scope boundaries and verifies corrective actions within approved scope.

Sources: N01 Assessing Security and Privacy Controls, N03 Guide to Operational Technology Security, P01 Adoption of utility IT cybersecurity regulations, D01 Cybersecurity Regulation Part 500

Evidence request and secure collection

The evidence request is written so the utility can answer it from records it already holds, and the collection is designed so that each customer's data stays in its controlled system while the control is proved.

Request package

Request the current charter and licenses, the PSC entity classification and service count definitions, the historic implementation plan, regulator letters and rubric, the last two audits and their corrective actions, DFS filings and exemptions, risk assessments, board approvals, asset, application and vendor lists, customer data flows, policies, access reviews, test reports, incident logs, exercise and restoration results, contracts and the retention schedule. Specify the period, the owner, the delivery date and the acceptable redactions for each item, and log the delivery status of each item with its effect on the conclusion.

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

Evidence record

Assign an evidence identifier to every item. Record the system or control, the custodian, the source record and period, the extraction method and filters, the collection timestamp with its time zone, an integrity value where useful, access restrictions, the controlled location, retention or hold and the linked sample identifiers. Preserve the original time data and explain any normalized display. Record who supplied a statement separately from who observed a result, because the two carry different weight when the finding is challenged.

Minimum necessary

Use aggregate counts, synthetic customer records, redacted screenshots and supervised displays wherever they are sufficient. The workbook stores controlled references, and a secure evidence repository is agreed before collection begins.

Regulator disclosure

Part 1200 confidentiality operates through the applicable disclosure exemptions, which are applied record by record. Follow the actual filing procedures for restricted material and involve the records and FOIL decision maker. Counsel decides how privilege is asserted, record by record, on the substance of each item.

Sources: P01 Adoption of utility IT cybersecurity regulations, D01 Cybersecurity Regulation Part 500, N01 Assessing Security and Privacy Controls, N02 Protecting PII confidentiality

---

Sampling and assessment conclusions

A conclusion carries the weight of the population behind it, and the sampling record is where an auditor tests whether the result means what the report says.

Define populations

For each test record the complete population, the period and the source. Examples include all privileged users across scoped systems, terminated workers in the period, active suppliers handling NPI, external customer data transfers, critical recovery services and known exceptions. Reconcile the source totals before selecting samples, and keep the reconciliation; a reconciled list is what ties the sample to the full population.

Select deliberately

For judgmental sampling, examine the high consequence systems, the emergency accounts, the exceptions, the material changes and the prior failures first, then representative ordinary records. State the counts and the selection reasons. If statistical sampling is used, obtain a qualified design and document confidence, precision and limitations separately. This pack leaves the sample size to the audit lead's stated rationale, which is the record that justifies it.

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

Expand on failure

A missing MFA policy is a design issue; an approved policy with an unprotected direct login is an operating failure, and the two are written up differently. Expand to related systems, users or providers when a failure could be systemic. Escalate evidence gaps and scope restrictions. A vendor assurance report is accepted as evidence once it matches the service, the period, the tests and the applicable customer responsibilities.

Use precise result states

Record Not examined, Evidence requested, Supported, Exception found or Not applicable with basis. A supplied narrative opens the test, and the evidence behind it decides the result. Record the condition, the criterion, the evidence, the sample extent and the test limitations.

Sources: N01 Assessing Security and Privacy Controls

Field procedure for billing, AMI and access

The billing, meter data and customer access systems hold the private information the regimes protect, and the field procedure examines them through supervised demonstrations with synthetic identities rather than through live customer data.

Before arriving

Confirm the target systems, the safe read only collection method, the escort, the expected baseline, the approved synthetic identities and the account roles. Check whether the meter platform or the historian interface can affect physical operations, because a metering head end with a disconnect capability is an operational system however it is labelled. Obtain explicit additional authority for any live authentication, export or connectivity demonstration.

Observe and record

Reconcile the billing, meter data management and AMI inventory identifiers to the approved diagrams. Ask the owner to show synthetic customer search, role masking, export authorization, consent enforcement and audit event capture, and record the method, the time, the user role, the expected and actual outcome and the evidence reference for each. Compare joiner, leaver and vendor access samples with the approval and revocation records; the revocation records are where the examiner looks hardest.

Protect operations

Check the relevant DNP3, Modbus, IEC 61850 or proprietary interface paths from engineering evidence where present; vulnerability is judged from that evidence, and any test runs on its own written authorization.

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

Stop and hand back

Stop on an unapproved target, an operational alarm, a latency change, an unexpected private record, disabled logging or an owner request. Notify the operating authority, record the condition and follow its recovery direction. Confirm the post work service state, remove only the approved temporary access and transfer the records through the controlled channel.

Sources: N03 Guide to Operational Technology Security, P01 Adoption of utility IT cybersecurity regulations

---

Field procedure for segmentation and recovery

Part 1200 asks a utility to be able to segment IT from OT in an incident, and the field procedure examines that capability from diagrams, rule exports and rehearsal while every cable stays connected.

Trace dependencies first

Map the shared identity, DNS, time, endpoint management, remote support, historians, backup services and manual fallback. Explain whether isolating IT could disrupt dispatch, alarms, customer assistance, outage management or recovery, because the shared identity directory is the dependency to trace first. Obtain the actual operating owner's acceptance of the method and the sequence.

Assess from records and rehearsal

Examine rule exports and diagrams, interview engineers and rehearse the isolation runbook on paper. Record the allowed and denied paths and the untested assumptions. Where stronger assurance is needed, propose representative laboratory validation or a separately authorized maintenance window test with precise targets, baselines, abort criteria, recovery steps and named authorities.

Verify service recovery

Inspect the evidence that the required identity, keys, application dependencies, data and supplier services can be restored in the necessary sequence. Restoration is evidenced by a completed restore, with the backup job log as the starting record. Distinguish tabletop, laboratory restoration, partial component test and full service recovery, and record the actual measured results beside the stated recovery objectives.

Exception handling

A technical safety constraint is met with a documented alternate method and a compliance decision, and the mandatory testing duty stays on the record for that decision. Carry untested paths and open legal acceptance into the findings and the adoption record, so a later reader sees the constraint and the decision together.

Sources: N03 Guide to Operational Technology Security, P01 Adoption of utility IT cybersecurity regulations, D01 Cybersecurity Regulation Part 500

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

Notification clocks, with each trigger kept separate

Regime	Trigger, action and limit
PSC 1200.21(a)	Covered entity: notify designated DPS director promptly, no later than 72 hours after reasonably believing a defined incident affecting covered IT/information, affiliate or third party provider occurred/is occurring. Check exact text and Q04.
DFS 500.17(a)	Covered entity: notify superintendent electronically promptly, no later than 72 hours after determining a defined cybersecurity incident occurred at entity, affiliate or TPSP. Keep material updates. Definition differs from PSC.
DFS 500.17(c)	For extortion payment connected with covered entity cybersecurity event: payment notice within 24 hours; reasons, alternatives and diligence description within 30 days of payment. Payment decision has separate sanctions/legal review.
GBL 899-aa(2),(3)	Owner/licensee: affected NY residents as expedient as possible, without unreasonable delay, within 30 days of discovery subject to lawful law enforcement delay. Maintainer: owner/licensee immediately with statutory 30 day outside limit.
STL 208(2),(3),(10)	State entity: most expedient/no unreasonable delay with statutory scope/restoration/LE context and ITS consultation. Maintainer: owner immediately. Local policy/law governs local agency route. Timing follows section 208's own standard.

Sources: P01 Adoption of utility IT cybersecurity regulations, D01 Cybersecurity Regulation Part 500, B01 Private information breach notification, B03 State and local breach notification duties

Incident threshold screen and escalation

Three regimes define an incident differently, and the screen records a separate determination, official and timestamp for each so the clocks can be shown to have started on the right facts.

PSC event and incident

Part 1200 defines events broadly, including unsuccessful access or disruption attempts and unauthorized NPI dissemination. Its incident definition includes an event with a reasonable likelihood of harming any normal operations; actual or imminent jeopardy to IT confidentiality, integrity, availability or business functioning; lost operational data; a ransom demand to restore IT access; dissemination of NPI; or an event otherwise triggering a government, regulatory or supervisory notice duty. Apply the full 1200.1(d) and (e) wording, and maintain the event and incident log for every event, including those outside the 72 hour notice.

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

DFS incident

Part 500.1(g) concerns events at the entity, an affiliate or a third party service provider that impact the covered entity and require notice to a government, self regulatory or supervisory body; have a reasonable likelihood of materially harming a material part of normal operations; or deploy ransomware within a material part of its information systems. A Part 1200 incident decision and a DFS incident decision can therefore differ, and each determination is kept with its official and timestamp.

Statutory breach

GBL 899-aa includes unauthorized access or acquisition and statutory conditions concerning private information, encryption, keys and good faith business access. STL 208(1)(b) uses acquisition wording while subdivision 2 refers to accessed or acquired information. Escalate this textual difference for interpretation, and keep access only evidence on the record while counsel reads the two definitions side by side.

Immediate internal action

A technician or analyst records the observed facts and notifies the designated incident authority promptly. Preserve evidence, protect service and follow the approved containment. Legal and compliance evaluate the parallel duties as the facts arrive, alongside the record count and the analysis report. If a trigger is uncertain, record the uncertainty, the next decision owner and the time, and keep every clock running while the question is answered.

Sources: P01 Adoption of utility IT cybersecurity regulations, D01 Cybersecurity Regulation Part 500, B01 Private information breach notification, B03 State and local breach notification duties

---

Resident notices and regulator coordination

Resident notice, agency notice and consumer reporting agency notice each have their own recipients, thresholds and content, and the execution record shows which was sent, when, by whom and against which facts.

GBL recipients and content

When New York residents are notified, notify the Attorney General, the Department of State and the State Police as to timing, content, distribution and the approximate affected count, and include the notice template, with resident notice going out on its own schedule. The statute also requires notice to the Department of Financial Services for covered entities under 23 NYCRR 500.17. More than 5,000 New York residents notified at one time triggers consumer reporting agency notice. Review the required notice contact details, data categories and permitted delivery method before the template is approved.

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

State route and local procedure

STL 208 uses Attorney General, Department of State and ITS recipients and consumer reporting agencies above its more than 5,000 threshold. Its 90 day ITS report is an ITS duty that follows notice, and the operator's notice runs on the statute's own timing. Local agencies retrieve their adopted policy or law and record the escalation route it prescribes.

Exceptions and alternative notices

Use the precise inadvertent authorized disclosure and harm conditions. Keep the written determination for 5 years; if over 500 New York residents are affected, provide it to the Attorney General within 10 days of the determination. Qualifying notice under another specified regime may stand in for duplicate resident notice, and the remaining agency and consumer reporting agency duties continue alongside it. HIPAA and HITECH related Attorney General notice provisions require separate assessment, including the 5 business day rule after HHS notice.

Execution

Verify the current authenticated channels before an incident, so they are ready when one occurs. Record the approver, the facts known and unknown, the legal basis, the timestamps, the submitted version, the receipt, the updates and the delivery exceptions. Contracts may require earlier supplier or insurer notice. The workbook creates the decision record, and the filing receipt is the evidence that the notice was made.

Sources: B01 Private information breach notification, B03 State and local breach notification duties, B04 Attorney General breach reporting, D01 Cybersecurity Regulation Part 500, P01 Adoption of utility IT cybersecurity regulations

---

Data access, consent and supplier agreements

Energy data access runs under its own orders, tariffs and agreements, and the examination tests a controlled disclosure end to end with synthetic data before it reads a single contract clause.

Scope the transaction

Cases 18-M-0376 and 20-M-0082 concern energy market and energy data access contexts. Establish the recipient, the data category, the purpose, the authorization, the applicable tariff and the executed agreement before choosing a checklist. Customer authorization, aggregated release and utility operational sharing can have different conditions, and each transaction type gets its own record.

Test a controlled disclosure

With synthetic data, follow the request to identity and authority validation, purpose and field limitation, consent and revocation, secure transfer, recipient access, logging and termination. Test a denied or revoked request as well as an approved one. Retain the actual agreement version, the applicable security attestation and the evidence of any exception approval.

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

Aggregation

Determine the current use case specific aggregation screen and later PSC clarifications, the approved data recipient and the re identification controls. The threshold comes from the current operative tariff and order set for the use case, which question Q07 retrieves before any release.

Contract examination

Check the required safeguards, remote and privileged access, incident notification, subcontractors, audit and evidence access, retention, return and destruction, legal holds and termination. A SOC report is evidence within its scope and period, and the examiner writes down how its controls map to the utility's regulatory audit duties and the recipient's contractual duties, so other evidence covers the rest.

Sources: P04 Minimum cybersecurity and privacy protections, P05 Data Access Framework order, P06 Data Access Framework clarification, P07 Public Service Law section 66, D06 Third party service provider risk guidance

---

Report, remediate and hand over

The report is written so that each statement in it can be traced to an evidence identifier, and the remediation record is kept so that a year later anyone can see what was fixed, what was verified and what was accepted.

Report structure

State the entities and period, the objectives, the controlling criteria, the scope and exclusions, the method, the population and sample extent, a summary of material risks, the findings, the unexamined areas, the notification decisions and the corrective actions. Separate legal duties, regulator interpretations, contract conditions and proposed good practice into their own sentences. Reference evidence identifiers rather than embedding private data in executive copies.

Correction process

Agree each finding's factual accuracy, and keep every evidence based result in the report as written. Assign an accountable owner, a target date, dependencies, resources and interim controls. Record the mandatory deadline separately from the proposed project target. Document rejected recommendations and the authority for residual risk decisions.

Verification

Collect implementation evidence and retest the failed condition with a safe approved method. Explain the population covered and any remaining exception. Close a finding when the criterion, the evidence and the verification decision support closure. Reopened failures and changed scope carry their full history forward.

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

Evidence Handover and Chain of Custody Transfer

The project manager confirms recipient access to the retained records, named owners of all open questions and actions, current notification contacts, the recurring calendar and the transition decisions. Obtain technical, compliance and operating acceptance with scope and date. Personal owner review and legal sign off are each established by an actual completed record.

Sources: N01 Assessing Security and Privacy Controls, P01 Adoption of utility IT cybersecurity regulations, D01 Cybersecurity Regulation Part 500

C01 and C02: Entity Boundary, Evidence and Sampling

C01 Legal entity and system boundary

Criterion: P01 1200.1(c); D01 500.1(e); B02 2(a); B03 1(c),10. Proposed procedure: Reconcile charter, ownership chart, operating agreements, PSC classification, DFS authorizations and NY resident data. Trace shared IT services to each entity. Record a separate decision for each duty.

Request: Charter and licenses; service counts with definition/date; entity to system map; signed applicability reasoning. Acceptance: Each determination rests on entity facts. A fact still being gathered is marked Unresolved. Owner: Compliance owner.

C02 Evidence and sampling plan

Criterion: N01 assessment planning; proposed audit method. Proposed procedure: Define period, populations and methods before selecting samples. Reconcile source totals. Include all high consequence systems and exceptions, then representative ordinary cases. Record selection rationale and expand on failure.

Request: Population counts, extraction provenance, sample IDs, exclusions and method permits. Acceptance: A judgmental sample supports conclusions about the items examined, and statistical or organization wide conclusions rest on a qualified statistical design. Owner: Audit lead.

Sources: P01 Adoption of utility IT cybersecurity regulations, D01 Cybersecurity Regulation Part 500, B02 Reasonable security safeguards, B03 State and local breach notification duties, N01 Assessing Security and Privacy Controls

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

C03 and C04: Data Flows and Safeguard Ownership

C03 Customer and workforce data flow

Criterion: B02 2(b); N02 identification guidance. Proposed procedure: Trace account opening through billing, meter ingestion, collection, support, payroll, vendor transfer, archive and destruction. Reconcile application and vendor inventories against data owner interviews. Use synthetic records.

Request: Data flow map with owner, purpose, categories, location, recipients and retention basis. Acceptance: PII, statutory private information and each NPI definition are classified separately. Each unmapped copy stays on the open list until it is traced. Owner: Privacy lead.

C04 Safeguard program ownership

Criterion: B02 2(b)(ii)(A). Proposed procedure: Inspect designated coordinator, internal/external risk assessment, training records, supplier selection and contracts. Trace a business change to a documented program adjustment.

Request: Appointment, risk register, training population, executed contracts and change review. Acceptance: Policy statements supported by actual period evidence; any safe harbor claim supported by evidence of the program, with registration as one record among several. Owner: CISO.

Sources: B01 Private information breach notification, B02 Reasonable security safeguards, N02 Protecting PII confidentiality, P01 Adoption of utility IT cybersecurity regulations

C05 and C06: Physical Access, Evidence and Incident Notices

C05 Physical access and evidence handling

Criterion: B02 2(b)(ii)(C); N02 safeguards. Proposed procedure: Walk approved rooms with escort. Compare badge permissions and visitor records with authorized roles. Inspect media transport and destruction controls through records and supervised observation, leaving live cabinets closed and personal data in place.

Request: Dated access samples, escort record, media chain and destruction certificates. Acceptance: Unauthorized access paths and missing disposal proof become findings; field access follows site safety rules. Owner: Field technician.

C06 Incident facts and parallel notice decisions

Criterion: B01 2-8; B03 2-7,10; D01 500.17; P01 1200.21. Proposed procedure: Record discovery, reasonable belief, determination and payment timestamps separately with timezone. Identify entity, data definition, affected residents, recipients and exceptions. Exercise escalation using a fictional incident.

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

Request: Trigger specific decision log, approved message, delivery receipts, updates and any lawful delay basis. Acceptance: Every applicable clock has a named official. An uncertain conclusion triggers escalation while the clock keeps running. Owner: Incident commander.

Sources: B02 Reasonable security safeguards, N02 Protecting PII confidentiality, N03 Guide to Operational Technology Security, B01 Private information breach notification, B03 State and local breach notification duties, D01 Cybersecurity Regulation Part 500, P01 Adoption of utility IT cybersecurity regulations

---

C07 and C08: Retention, Holds, Findings and Retest

C07 Retention and legal holds

Criterion: B02 2(a),(b)(ii)(C); B01 2(a); D01 500.6,500.13,500.17; P01 1200.6,1200.13,1200.21. Proposed procedure: Build schedule by record class and authority. Reconcile legal holds before deletion. Inspect a completed deletion and backup expiry sample. Keep audit log and certification retention separate.

Request: Approved schedule, hold register, disposal evidence and backup lifecycle settings. Acceptance: Three year or five year regulatory minima are applied as minimum retention for their record classes, with deletion dates set by the full schedule. P01 1200.13 cross reference is listed for clarification. Owner: Records manager.

C08 Finding, correction and retest

Criterion: N01 assessment results; proposed project method. Proposed procedure: For each finding state condition, criterion, evidence, extent and operational/privacy consequence. Assign owner/date and proposed remedy. Retest implemented changes with separate evidence and scope.

Request: Finding ID linked to evidence, action decision, change record and retest result. Acceptance: Implemented and Verified are separate states, and Verified follows the retest. Mandatory duties stay in force alongside any management risk acceptance entry. Owner: Audit lead.

Sources: B01 Private information breach notification, B02 Reasonable security safeguards, D01 Cybersecurity Regulation Part 500, P01 Adoption of utility IT cybersecurity regulations, N01 Assessing Security and Privacy Controls

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

P01 and P02: Executive Support, Policies and Privacy

P01 Executive support and governance

Criterion: 1200.18(a)(1),1200.2-1200.4. Proposed procedure: Inspect qualified CISO appointment, retained utility responsibility and senior oversight of outsourced services. Trace a material privacy risk from assessment through resources and leadership reporting.

Request: CISO remit, leadership minutes, budget decision and annual CISO report. Acceptance: Due requirements and transition status established. Leadership support evidenced beyond an unsigned policy. Owner: CISO.

P02 Policies and customer privacy

Criterion: 1200.18(a)(2),1200.3. Proposed procedure: Map all seventeen policy areas to adopted policies and operating procedures. Inspect approval and compare written promises to actual billing, AMI and support workflows.

Request: Approved policy matrix, procedures and handling samples. Acceptance: Every applicable area covered, including customer data segregation and incident IT/OT segmentation. Owner: Privacy lead.

Sources: P01 Adoption of utility IT cybersecurity regulations

P03 and P04: Network Security and Customer Data Segregation

P03 Network security and vulnerability program

Criterion: 1200.18(a)(3),1200.5. Proposed procedure: Examine network controls and evidence of effective continuous monitoring. If its exception is relied on, verify ongoing change/vulnerability detection. Otherwise check 12 month penetration and six month vulnerability assessments after transition.

Request: Monitoring coverage, detection cases, test scope, assessment dates and remediation records. Acceptance: Apply the current DFS requirement to current DFS 500.5, which sets annual penetration testing in place of the old continuous monitoring alternative. Any OT test runs under its own separate authorization. Owner: Technical lead.

P04 Customer data segregation and masking

Criterion: 1200.18(a)(4),1200.3(a)(13),1200.7(c). Proposed procedure: Trace billing and identifiable consumption data through approved access paths. Examine logical separation, exports, non production masking and least privilege views. Use approved synthetic accounts to demonstrate.

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

Request: Path diagram, role to field map, masking policy and test evidence. Acceptance: Document accessible data and bypasses. Owner: Technical lead.

Sources: P01 Adoption of utility IT cybersecurity regulations, N03 Guide to Operational Technology Security

---

P05 and P06: Training and Vendor Access

P05 Training and employee awareness

Criterion: 1200.18(a)(5),1200.14(b). Proposed procedure: Reconcile the personnel roster with annual training completion after transition. Check content against current assessment risks, contractor handling duties and social engineering. Interview designated responders.

Request: Roster denominator, completion exceptions, content version and escalation demonstration. Acceptance: Failures have owners. Owner: Security training owner.

P06 Vendor and consultant access

Criterion: 1200.18(a)(6),1200.11,1200.12. Proposed procedure: Reconcile third parties and affiliates. Trace provisioning, approval, MFA or written equivalent approval, expiry and revocation for support, billing and remote maintenance.

Request: Provider register, contracts, named access samples, review and termination evidence. Acceptance: Accounts traceable to people and scope. Affiliate treatment follows Part 1200 policy even though its TPSP definition excludes affiliates. Owner: Vendor owner.

Sources: P01 Adoption of utility IT cybersecurity regulations, P03 PII implementation plan order

---

P07 and P08: Physical Security, Response and Drills

P07 Physical security of data systems

Criterion: 1200.18(a)(7),1200.3(a)(10). Proposed procedure: Inspect sites holding customer data, including branch offices, print operations and approved hosting assurance. Reconcile visitor controls, privileged console access and media disposal.

Request: Access roster samples, visitor logs, exception approvals and disposal proof. Acceptance: Off site supplier controls are covered by evidence with a stated scope. Owner: Facilities owner.

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

P08 Response, recovery and drills

Criterion: 1200.18(a)(8),1200.16. Proposed procedure: Examine all eleven plan subjects. Review yearly exercise simulating breach and NPI compromise, then trace required plan updates within 90 days. Confirm incident and recovery roles can access plans during outages.

Request: Exercise decisions, update dates, recovery dependency map and approved communications. Acceptance: Tabletop evidence described as a simulation. Any statement that backups restore service rests on restoration evidence. Owner: Recovery owner.

Sources: P01 Adoption of utility IT cybersecurity regulations

---

P09 and P10: Supply Chain and IT to OT Segmentation

P09 Supply chain and third party risk

Criterion: 1200.18(a)(9),1200.11. Proposed procedure: Examine vendor and affiliate risk evaluation, minimum practices, due diligence and biennial policy reassessment. Trace a high risk provider through contract, change, monitoring and exit.

Request: Risk tier rationale, assessed evidence, contract controls, subcontractor dependencies and exit plan. Acceptance: Assurance period and service coverage verified. A report logo or questionnaire opens the review, and assessed evidence completes it. Owner: Vendor owner.

P10 IT to OT incident segmentation

Criterion: 1200.18(a)(10),1200.3(a)(17),1200.16(b)(10). Proposed procedure: Use approved diagrams and rule exports to map identity, DNS, jump hosts, time, historians and shared recovery dependencies. Walk through a controlled isolation decision. Test in a representative lab or separate approved window.

Request: Dependency map, isolation runbook, authority, baseline, stop conditions and restoration record. Acceptance: Document review authority covers diagrams, exports and walkthroughs; any live disconnection or active OT scan runs in its own approved window. Record untested paths and service consequences. Owner: OT operating owner.

Sources: P01 Adoption of utility IT cybersecurity regulations, N03 Guide to Operational Technology Security

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

P11 and P12: Part 1200 Certification and Forensic Readiness

P11 All Part 1200 duties and certification

Criterion: 1200.18(a)(11),1200.17-1200.25. Proposed procedure: Reconcile the complete obligation matrix, phase in schedule, yearly qualified third party audit available by September 15, staff requests, notification readiness and June 30 certification from 2027. Resolve first year timing with DPS.

Request: Clause matrix, audit scope, auditor qualifications, request log, certificate support and submission receipts. Certification rests on the clause matrix and its supporting evidence. Owner: Compliance owner.

P12 Forensic and credit monitoring readiness

Criterion: 1200.19,1200.20. Proposed procedure: Inspect executed forensic vendor and credit monitoring contracts. Verify response capability, investigative reporting and credit service capabilities. Exercise an offer covering at least one year from offer when GBL resident notice is required.

Request: Contract terms, activation route, capacity, covered capabilities and offer/payment arrangements. Acceptance: Retainer represented as readiness, with completed incident work evidenced by its own report. Duty subject to transition and actual incident facts. Owner: Incident commander.

Sources: P01 Adoption of utility IT cybersecurity regulations, P02 Notice of adoption of Part 1200, B01 Private information breach notification

D01 and D02: DFS Coverage, Class A and Governance

D01 DFS coverage, exemption and Class A

Criterion: 500.1(d),(e),500.19. Proposed procedure: Verify license or required authorization for each entity. Calculate Class A metrics using the correct affiliate sharing rules. Test exemption criteria and preserve filing evidence. Identify duties retained by a partial exemption.

Request: License record, group calculations, section level exemption matrix and filed notice. Acceptance: Each exemption rests on the section 500.19 criteria and the filed notice. A partial exemption retains specified controls and notices. Owner: Compliance owner.

D02 Program, policies and governing body

Criterion: 500.2-500.4. Proposed procedure: Inspect annual policy approval, CISO appointment, annual written report and timely material issue escalation. Trace governing body oversight, understanding and resources to actual decisions.

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

Request: Policy approval, CISO reports, material issue records and oversight minutes. Acceptance: Adopting affiliate controls retains entity accountability and examination access. Apply actual exemptions. Owner: CISO.

Sources: D01 Cybersecurity Regulation Part 500, D02 Cybersecurity resource center, D03 Requirements by exemption and entity category, D07 Adopting an affiliate cybersecurity program

---

D03 and D04: Risk Assessment and Application Security

D03 Risk assessment and treatment

Criterion: 500.9; September 2026 DFS guidance. Proposed procedure: Reconcile scope to inventory, NPI flows, business processes, cloud and third parties. Inspect annual review/update and material change updates. Trace threat, vulnerability, control evidence and residual risk to treatment decisions.

Request: Method criteria, assessment, control linkage, named treatment owners and approval. Acceptance: Systems outside the assessment and residual risk conclusions awaiting support stay visible on the record. Guidance good practices labeled separately. Owner: Risk manager.

D04 Vulnerability and application security

Criterion: 500.5,500.8. Proposed procedure: Check annual inside/outside penetration testing, risk based automated scans plus manual review for systems not scanned and material change assessment. Examine secure development and at least annual CISO/designee procedure review.

Request: Qualified test reports, scope, scan/manual coverage, change triggers and SDLC reviews. Acceptance: Current DFS annual penetration testing is performed alongside any continuous monitoring. Unsafe OT gaps escalated for a compliant approved method. Owner: Technical lead.

Sources: D01 Cybersecurity Regulation Part 500, D05 Risk assessment guidance, N03 Guide to Operational Technology Security

---

D05 and D06: Access, MFA, Inventory and Class A Controls

D05 Access, MFA and inventory

Criterion: 500.7,500.12,500.13(a). Proposed procedure: Reconcile user, privileged and service accounts to system inventory. Review annual privileges and prompt leaver termination. Trace MFA coverage, direct login bypasses and written compensating controls with annual review.

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

Request: Access population, inventory owner/location/classification/support/RTO, MFA paths and exceptions. Acceptance: Limited exemption MFA has its own scope. Public informational websites evaluated under the current DFS FAQ guidance on customer login. Owner: Identity owner.

D06 Class A additional controls

Criterion: 500.2(c),500.7(c),500.14(b). Proposed procedure: If Class A applies, inspect risk based independent audit, privileged activity monitoring, PAM and common password blocking, EDR and centralized security alerting. Validate precise exception conditions per clause.

Request: Class determination, audit independence, coverage maps and written clause specific approvals. Acceptance: Set the Class A audit frequency from the risk assessment, separately from the PSC yearly audit, and apply each exception to the controls it names. Owner: Audit lead.

Sources: D01 Cybersecurity Regulation Part 500, D04 Cybersecurity frequently asked questions, D03 Requirements by exemption and entity category

---

D07 and D08: Third Parties, Encryption, Logs and Training

D07 Third parties and shared services

Criterion: 500.11 and affiliate program adoption. Proposed procedure: Assess providers through selection, contractual controls, ongoing review and exit. Review breach notice, access/MFA, encryption, subcontractors and evidence access. Trace adopted affiliate program to covered entity duties.

Request: Provider inventory, contracts, assurance scope, follow up, exit evidence and affiliate agreement. Acceptance: The covered entity keeps accountability for outsourced functions. Guidance recommendations recorded as good practice, separate from regulatory duties. Owner: Vendor owner.

D08 Encryption, logs and training

Criterion: 500.6,500.14,500.15. Proposed procedure: Inspect external transit and at rest encryption coverage. Review written CISO approval for infeasible at rest encryption and annual review. Check financial reconstruction records at least five years, relevant security trails three years, and annual training incl social engineering.

Request: Configuration evidence, written exceptions, retention test and training roster. Acceptance: Transit encryption assessed under DFS 500.15 on its own terms, separate from the PSC alternatives. Retention minima applied to defined record classes. Owner: Technical lead.

Sources: D01 Cybersecurity Regulation Part 500, D06 Third party service provider risk guidance, D07 Adopting an affiliate cybersecurity program

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

D09 and B01: Resilience, Notices and Private Information

D09 Resilience and notices

Criterion: 500.16,500.17. Proposed procedure: Review yearly response/BCDR testing and restoration testing. Check protected backups and critical suppliers. Exercise 72 hour incident reporting, payment related 24 hour/30 day notices and April 15 certification or acknowledgment.

Request: Restore results, response roles, trigger timestamps, update log and signed filing support. Acceptance: Highest executive and CISO or responsible senior officer sign actual required filing. Certification follows the signed filing support. Owner: Incident commander.

B01 Current private information classification

Criterion: GBL 899-aa(1); STL 208(1). Proposed procedure: Compare actual data categories with each statute. Include online account credentials and GBL medical/health insurance additions. Evaluate encryption and key compromise conditions. Keep usage data confidentiality and PSC NPI separate.

Request: Category by authority matrix with data owner and classification basis. Acceptance: Each PII category is classified under the statute that governs it, GBL or STL. Owner: Privacy lead.

Sources: D01 Cybersecurity Regulation Part 500, B01 Private information breach notification, B03 State and local breach notification duties, P01 Adoption of utility IT cybersecurity regulations, P07 Public Service Law section 66

B02 and B03: Business and Government Breach Notices

B02 Business breach notice and exceptions

Criterion: GBL 899-aa(2)-(8). Proposed procedure: Exercise resident notice as expedient as possible without unreasonable delay and within 30 days of discovery, subject to lawful law enforcement delay. Verify owner notice immediately for maintained data and the statutory outer limit.

Request: Discovery facts, notice content/method, recipients and actual delivery records. Acceptance: Notice moves as soon as the facts allow, within the 30 day outer limit, while forensics continues. Exceptions documented individually. Owner: Legal and incident lead.

B03 State and municipal notification procedures

Criterion: STL 208(1)(c),(2),(3),(7),(10). Proposed procedure: For a state entity apply its notification and ITS consultation procedure. For a local agency retrieve the required local policy/law and check consistency with section 208. Resolve charter and GBL overlap with counsel.

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

Request: Charter analysis, adopted local policy, state consultation records and recipient matrix. Acceptance: State entity classification follows the charter and function analysis. Municipal timing follows the adopted local policy or law. Owner: Compliance owner.

Sources: B01 Private information breach notification, B04 Attorney General breach reporting, B03 State and local breach notification duties

---

B04 and B05: Other Notice Regimes and Utility Data Sharing

B04 Inadvertent disclosure and other notice regimes

Criterion: GBL 899-aa(2)(a),(b),(8),(9); STL 208(2)(a),(b),(9). Proposed procedure: Test the exact inadvertent disclosure exception and required harm analysis. Retain written determination five years and notify AG within ten days of determination if over 500 NY residents. Evaluate qualifying alternative resident notices and continuing agency duties.

Request: Written decision, resident count, legal basis, retained copy and notices/receipts. Acceptance: More than 500 and more than 5,000 thresholds are distinct. HIPAA and DFS notices are assessed regime by regime against each NY notification duty. Owner: Legal lead.

B05 Utility data sharing and consent

Criterion: PSL 66(32); cases 18-M-0376 and 20-M-0082. Proposed procedure: Map identifiable, aggregated and public energy data to the specific use case, authorization, tariff and agreement. Test consent scope/revocation, recipient access and a denied transfer. Retrieve later amendments before applying aggregation thresholds.

Request: Current tariff/DSA, consent artifact, disclosure/denial logs and re identification assessment. Acceptance: Apply each aggregation rule to its own data type, and confirm the rule that governs each water sector exchange before applying energy market terms. Owner: Privacy lead.

Sources: B01 Private information breach notification, B03 State and local breach notification duties, P04 Minimum cybersecurity and privacy protections, P05 Data Access Framework order, P06 Data Access Framework clarification, P07 Public Service Law section 66

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

Control procedure B06 for sensitive customer and employee workflows

B06 Sensitive customer and employee workflows

Criterion: B02 safeguards; N02 context based PII protection. Proposed procedure: Trace medical hardship, assistance eligibility, payment scans, account recovery, call recordings and workforce records. Inspect purpose limits, role masking, test data practices and deletion holds. Use synthetic specimens.

Request: Restricted category inventory, approved role views, recovery verification and disposal evidence. Acceptance: Actual private data stays in its controlled system, with references in the workbook. HIPAA coverage decided on its own test, separate from the presence of medical categories. Owner: Privacy lead.

Sources: B01 Private information breach notification, B02 Reasonable security safeguards, N02 Protecting PII confidentiality

P13 and P14: Application Security and Risk Criteria

Use these procedures with the clause matrix and the applicable transition, exemption and current entity instructions. They supplement the original test sequence.

P13 Application security

P01 1200.8. Reconcile in house and external applications to the utility inventory. Inspect secure development and externally developed application evaluation procedures; trace an actual release and verify CISO/designee review at least every two years after transition.

Expected evidence: Application inventory, adopted SDLC, supplier evaluations, release evidence and dated review

Conclusion boundary: Evaluate both in house and externally developed software. Record scope and transition. Proposed owner: Application owner. Actual results and reviewer are recorded at execution.

P14 Risk assessment criteria and updates

P01 1200.9. Inspect the written assessment method, risk categories, control adequacy and mitigation/acceptance criteria. Reconcile systems and data to scope. Verify at least biennial assessment and reasonably necessary change updates after transition.

Expected evidence: Assessment, method, inventory reconciliation, change register and treatment decisions

Conclusion boundary: Actual scope and evidence support risk conclusions. Each score is traced to its scope and evidence. Proposed owner: Risk manager. Actual results and reviewer are recorded at execution.

Sources: P01 Adoption of utility IT cybersecurity regulations

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

P15 and P16: Qualified Personnel, Intelligence and Encryption

Use these procedures with the clause matrix and the applicable transition, exemption and current entity instructions. They supplement the original test sequence.

P15 Qualified personnel and intelligence

P01 1200.10. Reconcile required cybersecurity functions with qualified staffing and provider responsibilities. Inspect training, updates and verification of key personnel knowledge. Test escalation of relevant intelligence to an accountable owner.

Expected evidence: Role/competence records, resource decisions, updates and escalation sample

Conclusion boundary: Assigned staff and suppliers can perform or oversee their scoped duties. Proposed owner: CISO. Actual results and reviewer are recorded at execution.

P16 Encryption and approved alternatives

P01 1200.15. Map NPI at rest and in external transit. Inspect effective encryption or documented infeasibility and CISO approved compensating controls. Verify at least yearly feasibility/effectiveness review when alternatives are used.

Expected evidence: Data flow, configurations, approved alternatives and annual review

Conclusion boundary: PSC alternatives and transition apply to PSC duties, and DFS transit encryption follows its own requirements. Proposed owner: Technical lead. Actual results and reviewer are recorded at execution.

Sources: P01 Adoption of utility IT cybersecurity regulations

D10 and D11: Qualified Personnel and Regulator Access

Use these procedures with the clause matrix and the applicable transition, exemption and current entity instructions. They supplement the original test sequence.

D10 Qualified personnel and intelligence

D01 500.10. Inspect qualified staffing/oversight of cybersecurity functions, current knowledge and training. Reconcile outsourced roles with retained entity responsibilities.

Expected evidence: Role competence, training, supplier agreement and oversight records

Conclusion boundary: Exemptions and actual function boundaries are evidenced. Proposed owner: CISO. Actual results and reviewer are recorded at execution.

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

D11 Regulator access and electronic submission

D01 500.18,500.24. Verify authorized electronic filing channels, retained submission receipts and any written superintendent approved exemption. Demonstrate controlled retrieval of relevant examination records with secrets kept protected.

Expected evidence: Filing procedures, authorizations, receipts and written exceptions

Conclusion boundary: Filings and exemptions evidenced by their submission receipts. Proposed owner: Compliance owner. Actual results and reviewer are recorded at execution.

Sources: D01 Cybersecurity Regulation Part 500

Adoption worksheet

Save completed worksheets in the approved controlled location. Use evidence references and synthetic examples; keep customer data and system secrets out of these fields.

Evidentiary Record Fields

Legal entity, ownership, jurisdiction and controlled record reference

Systems, business processes, period and exclusions

Sponsor, technical, compliance and operating approval names, dates and limits

---

Applicability decision worksheet

Save completed worksheets in the approved controlled location. Use evidence references and synthetic examples; keep customer data and system secrets out of these fields.

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

Evidentiary Record Fields

Instrument, version, effective dates and clause

Entity facts, evidence IDs, thresholds and exceptions

Decision, reasoning, reviewer, date and unresolved clarification

---

Field activity authorization

Save completed worksheets in the approved controlled location. Use evidence references and synthetic examples; keep customer data and system secrets out of these fields.

Evidentiary Record Fields

Exact target, method, operator, window and evidence location

Baseline, stop criteria, safety restrictions and recovery authority

Approval before activity, actual observations, stop/recovery record and operating handback

---

Finding and retest worksheet

Save completed worksheets in the approved controlled location. Use evidence references and synthetic examples; keep customer data and system secrets out of these fields.

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

Evidentiary Record Fields

Condition, criterion, evidence, population/sample extent and consequence
Owner, remedy, mandatory deadline, project target and interim controls
Implemented evidence, verification method/results, remaining limits and closure authority

---

Notification decision worksheet

Save completed worksheets in the approved controlled location. Use evidence references and synthetic examples; keep customer data and system secrets out of these fields.

Evidentiary Record Fields

Entity, information category, discovery, reasonable belief, determination and payment times with timezone
Applicable triggers, recipients, time limits, exception basis, approver and unresolved issues
Approved notice version, delivery/receipt times, continuing updates and retained evidence

---

Sources P01 to B03: PSC, DFS and Breach Statutes

P01 Adoption of utility IT cybersecurity regulations

NYS Public Service Commission. Final adoption order and adopted text. Case 25-M-0302, April 17 2026; Appendix A, sections 1200.0-1200.26 and Appendices 18-19. Use the adopted definitions for exact customer counts. Apparent cross reference errors and first year scheduling are listed for clarification.

D01 Cybersecurity Regulation Part 500

NYS Department of Financial Services. Agency hosted regulation reading copy. Second amendment, November 1 2023; sections 500.1-500.24. The cover identifies the codified text as the official version. Reconcile the operative codified text and later amendments before a signed legal conclusion.

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

B01 Private information breach notification

New York State Senate. Current statute text. GBL 899-aa, revision March 28 2025, subdivisions 1-10. Use current medical/health insurance additions, access or acquisition trigger and 30 day outside limit. Read separately from STL 208.

B02 Reasonable security safeguards

New York State Senate. Current statute text. GBL 899-bb, subdivisions 1-2. Compliant regulated entity requires both applicability and compliance. Small business means safeguards tailored to the business's size and complexity.

B03 State and local breach notification duties

New York State Senate. Current statute text. State Technology Law 208, subdivisions 1(c), 2, 3, 7 and 10. Local agencies excluded from state entity definition but have a local notification policy duty.

Sources: P01 Adoption of utility IT cybersecurity regulations, D01 Cybersecurity Regulation Part 500, B01 Private information breach notification, B02 Reasonable security safeguards, B03 State and local breach notification duties

---

Sources N01 to D03, DFS instruments and NIST guidance

N01 Assessing Security and Privacy Controls

NIST. Final technical guidance. SP 800-53A Rev. 5; assessment planning and examine/interview/test; release 5.2.0 noted August 27 2025. A method for tailoring assessment procedures, used here as audit practice alongside the NY legal criteria.

N03 Guide to Operational Technology Security

NIST. Final technical guidance. SP 800-82 Rev. 3, September 2023, OT safety and assessment tailoring. Part 1200 excludes OT from IT, while requiring IT/OT segmentation capability. Part 500 information systems can include industrial controls when in scope.

D05 Risk assessment guidance

NYS Department of Financial Services. Agency guidance. September 10 2026; governance, scope, methodology and treatment. Explains required risk assessment use and good practices. Its good practices are read alongside the regulation's existing duties.

D02 Cybersecurity resource center

NYS Department of Financial Services. Agency guidance and current resource index. Covered entities, regulation and submissions links. DFS coverage follows the entity's license or authorization. Guidance is read alongside the regulation it explains.

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

D03 Requirements by exemption and entity category

NYS Department of Financial Services. Agency guidance. Small business, other limited exemptions, standard and Class A tables. Use the actual regulation for definitions and exact subsection numbering.

Sources: N01 Assessing Security and Privacy Controls, N03 Guide to Operational Technology Security, D05 Risk assessment guidance, D02 Cybersecurity resource center, D03 Requirements by exemption and entity category

---

Sources D07 to N02: PSC, DFS and NIST Guidance

D07 Adopting an affiliate cybersecurity program

NYS Department of Financial Services. Agency guidance. October 22 2021; responsibility and examination access. Older subsection references predate the 2023 amendment. Covered entity retains responsibility.

P08 Public utility definitions

New York State Senate. Current statute text. Subdivisions 11, 13, 23 and 26. Map the actual legal entity and its function.

P09 Small business definition

New York State Senate. Current statute text. Subdivision 8. For the Part 1200 gas exclusion: NY residence, independent ownership/operation and 100 or fewer employees. DFS and SHIELD use their own thresholds.

P07 Public Service Law section 66

New York State Senate. Current statute text. Subdivisions 19, 30 and 32. Commission powers and gas/electric consumption confidentiality. NERC CIP and Part 500 coverage are each decided on their own tests.

N02 Protecting PII confidentiality

NIST. Final technical guidance. SP 800-122, April 2010, identification, impact, safeguards and response. Federal agency guidance adapted as audit practice.

Sources: D07 Adopting an affiliate cybersecurity program, P08 Public utility definitions, P09 Small business definition, P07 Public Service Law section 66, N02 Protecting PII confidentiality

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

Sources P03 to P04: PSC Orders, DFS and Breach Statutes

P03 PII implementation plan order

NYS Public Service Commission. Final order. Case 13-M-0178, August 19 2013, pages 3-9. Directed large electric, gas and water utilities. Retrieve the named utility implementation plan and current staff instructions. Recommendations, operative directions and current replacement rules are each mapped on their own.

P02 Notice of adoption of Part 1200

NYS Department of State. Final adoption notice. May 6 2026 State Register, printed pages 2-3; PSC-27-25-00021-A, filing 332. Confirms June 1 2026 effective date. Its summary uses rounded customer language; use P01 for exact service connection and service line criteria.

D04 Cybersecurity frequently asked questions

NYS Department of Financial Services. Agency interpretation. Third parties, MFA, SSO, cloud and public facing systems. Separate interpretive examples from the operative rule. Anonymous informational sites are assessed for customer MFA under the FAQ's own examples.

B04 Attorney General breach reporting

NYS Office of the Attorney General. Official reporting portal. Report a data breach and SHIELD resources. Check the current submission instructions and all other required recipients.

P04 Minimum cybersecurity and privacy protections

NYS Public Service Commission. Final order. Cases 18-M-0376 et al., October 17 2019, discussion and adopted Data Security Agreement. Energy market data access relationships, applied to the vendors within that scope. Check later amendments and the executed agreement.

Sources: P03 PII implementation plan order, P02 Notice of adoption of Part 1200, D04 Cybersecurity frequently asked questions, B04 Attorney General breach reporting, P04 Minimum cybersecurity and privacy protections

Sources P05 to D06: PSC Orders and DFS Instruments

P05 Data Access Framework order

NYS Public Service Commission. Final order. Case 20-M-0082, April 15 2021, order and Appendix A. Data access classes, customer authorization and aggregation are checked against later orders, the actual use case and current tariff.

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

P06 Data Access Framework clarification

NYS Public Service Commission. Final order. Case 20-M-0082, November 18 2021, clarification and tariff modifications.

D06 Third party service provider risk guidance

NYS Department of Financial Services. Agency guidance. October 21 2025; selection through termination. Expressly framed as guidance within the existing Part 500 obligations. Distinguish recommendations from Part 500 mandates.

Sources: P05 Data Access Framework order, P06 Data Access Framework clarification, D06 Third party service provider risk guidance

---

Put a Court Qualified Examiner Beside Your Audit Team

This manual sets the sequence, the records and the stop conditions. Whether Part 1200 or Part 500 reaches your entity, when your first audit must be available and how the Q01 to Q10 items resolve for your utility are answered from the adopted text, written regulator direction and the facts of your ownership and systems, and the record of how you reached them is what an auditor will ask to see.

Global Digital Forensics has served counsel and businesses since 1992 with court tested and certified examiners. We help a utility team define the audit boundary, document the IT and OT dependencies an auditor will ask about, and prepare the forensic readiness arrangements that Part 1200 anticipates, while the utility and its advisers keep the applicability and certification decisions. Discuss your audit boundary or call (800) 868-8189. The first consultation is free. To see how we support a covered utility through the audit itself, read Utility Cybersecurity Audit Support and Incident Readiness.

Web Addresses for the Sources Cited

1. P01 Adoption of utility IT cybersecurity regulations: https://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId=%7B50419C9D-0000-C957-89B7-5F83A397191B%7D
2. D01 Cybersecurity Regulation Part 500: https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500
3. B01 Private information breach notification: https://www.nysenate.gov/legislation/laws/GBS/899-AA
4. B02 Reasonable security safeguards: https://www.nysenate.gov/legislation/laws/GBS/899-BB
5. B03 State and local breach notification duties: https://www.nysenate.gov/legislation/laws/STT/208
6. N01 Assessing Security and Privacy Controls: https://csrc.nist.gov/pubs/sp/800/53/a/r5/final
7. N03 Guide to Operational Technology Security: https://csrc.nist.gov/pubs/sp/800/82/r3/final
8. D05 Risk assessment guidance: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20260910-cyber-risk-assessment
9. D02 Cybersecurity resource center: https://www.dfs.ny.gov/cybersecurity
10. D03 Requirements by exemption and entity category: https://www.dfs.ny.gov/cybersecurity/requirements
11. D07 Adopting an affiliate cybersecurity program: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211022_affiliates_cybersecurity_program
12. P08 Public utility definitions: https://www.nysenate.gov/legislation/laws/PBS/2

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

13. P09 Small business definition: https://www.nysenate.gov/legislation/laws/SAP/102
14. P07 Public Service Law section 66: https://www.nysenate.gov/legislation/laws/PBS/66
15. N02 Protecting PII confidentiality: https://csrc.nist.gov/pubs/sp/800/122/final
16. P03 PII implementation plan order: https://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId=%7B5986D197-87DB-4D21-A89B-95DC45E05061%7D
17. P02 Notice of adoption of Part 1200: https://dos.ny.gov/system/files/documents/2026/05/050626.pdf
18. D04 Cybersecurity frequently asked questions: https://www.dfs.ny.gov/cybersecurity/faqs
19. B04 Attorney General breach reporting: https://ag.ny.gov/resources/organizations/data-breach-reporting
20. P04 Minimum cybersecurity and privacy protections: https://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId=%7B67FED85B-7A21-43AE-88D6-6633BFE66F24%7D
21. P05 Data Access Framework order: https://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId=%7BA228D385-3E0E-41BC-A433-8ABD62F8A6E4%7D
22. P06 Data Access Framework clarification: https://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId=%7BC6B5140A-F841-4718-ADA9-32A9AD54FBBE%7D
23. D06 Third party service provider risk guidance: https://www.dfs.ny.gov/industry-guidance/industry-letters/il20251021-guidance-managing-risks-third-party

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