New York utility cybersecurity and privacy audit planning pack

Planning edition October 16, 2026

NYDFS Part 500, PSC utility IT cybersecurity and customer privacy, and New York private-information safeguards and notification

Project use

Establish the entity-specific duties, plan a safe assessment, collect traceable evidence, assign corrections and verify closure. Includes procedures for cybersecurity managers, CISOs, privacy and risk managers, project managers and field technicians.

Working records

Use the editable audit workbook and the fillable worksheets. Read the companion review findings and unresolved authority questions before adopting the planning edition. Save completed records in the approved controlled location.

Adoption

Applicability decisions and approvals require actual utility facts, controlling instruments and named reviewers. The planning edition does not establish a utility compliance outcome. Website profile selections remain declared, unverified facts.

Contents

Select a section title to go to that page. Source references in the text open the issuing authority or publisher.

4 Start here: choose the audit boundary
5 Using the corrected workbook edition
6 Executive decisions and audit outputs
7 Applicability: DFS and shared services
8 Applicability: PSC Part 1200
9 Applicability: personal information and ownership
10 Data definitions: classify before testing
11 The 2013 PII order and current audits
12 Part 1200 transition and recurring calendar
13 Recurring duties after transition
14 DFS audit timing and filing differences
15 Plan the project and establish authority
16 Responsibilities and acceptance gates
17 Evidence request and secure collection
18 Sampling and assessment conclusions
19 Field procedure: billing, AMI and access
20 Field procedure: segmentation and recovery
21 Notification clocks: keep triggers separate
22 Incident threshold screen and escalation
23 Resident notices and regulator coordination
24 Data access, consent and supplier agreements
25 Report, remediate and hand over
26 Control procedures C01 to C02
27 Control procedures C03 to C04
28 Control procedures C05 to C06
29 Control procedures C07 to C08
30 Control procedures P01 to P02
31 Control procedures P03 to P04
32 Control procedures P05 to P06
33 Control procedures P07 to P08
34 Control procedures P09 to P10
35 Control procedures P11 to P12
36 Control procedures D01 to D02
37 Control procedures D03 to D04
38 Control procedures D05 to D06
39 Control procedures D07 to D08

Contents continued

Select a section title to go to that page. Source references in the text open the issuing authority or publisher.

40 Control procedures D09 to B01
41 Control procedures B02 to B03
42 Control procedures B04 to B05
43 Control procedures B06 to B06
44 Additional control procedures P13 to P14
45 Additional control procedures P15 to P16
46 Additional control procedures D10 to D11
47 Adoption worksheet
48 Applicability decision worksheet
49 Field activity authorization
50 Finding and retest worksheet
51 Notification decision worksheet
52 Sources and instrument status
53 Sources and instrument status
54 Sources and instrument status
55 Sources and instrument status
56 Sources and instrument status

Start here: choose the audit boundary

First decisions

Identify each legal entity, the services it performs, its customers and employees, the systems under review and the review period. A holding company, utility operating company, licensed insurance affiliate and operating contractor can have different obligations while sharing systems.

Use the records in sequence

Complete Applicability before treating a 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.

Stop conditions

Do not interpret an unresolved applicability answer as an exemption. Do not sign a compliance certificate from this workbook. No website selection authorizes access to a utility system, collection of private information or live testing.

What this edition 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 must complete the audit basis. The open-question report identifies material gaps.

Sources: P01, D01, B01, B02, B03.

Using the corrected workbook edition

Edition 2026-10-16-r2 adds structured execution records and separates evidence gaps from supported conclusions.

Before execution

Use all applicable procedures in the 41-row Control tests register. Freeze the exact criterion, population, review period, sample rationale and permitted method. Record actual execution dates, observations, evidence IDs and review. A proposed procedure or mapped clause is not an assessment result. Keep operating permission separate from a compliance criterion.

Open and incomplete decisions

The open count includes blanks, invalid decision text and resolved selections missing required record fields. Fields present still requires qualified review. Actual approvals remain uncompleted until the responsible people review the work.

Scope and authority

Record every proposed exclusion, reason and proposed responsible reviewer in Scope decisions. The builder preserves deferred task/test IDs and the full 469-record PSC/DFS clause and context matrix. Examine the exact source text, entity scope, period, decision evidence and mapped test before recording an actual conclusion. Definitions, administrative provisions and appendix forms have distinct labels. The operative DFS version, utility-specific criteria and Q01-Q10 still require resolution.

Source access and revision

Sources list retrieval status and available snapshot hashes. A restricted URL is not proof that a duty does not exist. Edition record tracks actual project revisions and reviews. Retain the previous edition and do not treat a template publication as a personal technical or legal approval.

Sources: N01, N03.

Executive decisions and audit outputs

Sponsor decisions

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

Required work products

The final project record should include a signed applicability matrix, approved scope and method permits, population and sample schedules, evidence index, criterion-level results, findings, corrective action decisions, retest results, notification decisions and a recurring-duty calendar. The executive report identifies material service and privacy risks, unresolved scope and decisions requiring resources.

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?

Risk decisions

Use the utility approved risk criteria. Record likelihood rationale, consequence, existing controls, uncertainty and residual exposure. A sponsor may prioritize investment or accept a residual business risk within authority. That entry cannot waive a law, rule, order, permit or contract.

Sources: N01, D05.

Applicability: DFS and shared services

Direct DFS coverage

Part 500 covers persons operating under or required to operate under qualifying Banking Law, Insurance Law or Financial Services Law authorizations. Operating an electric, gas, steam or water utility alone does not establish this status. Retrieve the actual license or required-authorization analysis, legal name and regulator record.

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 and exact period.

Partial exemptions

Section 500.19(a) uses alternative employee/contractor, revenue or asset tests, with distinct affiliate and period rules. Review the full section rather than selecting the most favorable number. An exemption from some provisions does not remove retained obligations such as applicable risk assessment, access, MFA, inventory, training and notices. File the required exemption notice and monitor changes.

Utility affiliate examples

A utility group with a separately DFS-licensed captive or other licensed affiliate needs an entity-level decision, not a group-wide assumption. Adopting the parent's program retains covered-entity responsibility and DFS evidence access. A utility acting only as a supplier may have contractual security duties without becoming a covered entity solely from that supply relationship.

Sources: D01, D02, D03, D07.

Applicability: PSC Part 1200

Use the final adopted definition in section 1200.1(c), not a press-release statement about 50,000 customers.

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). At 50,000 such connections the exclusion still applies.
Electric exclusion	Electric corporation maintaining fewer than 50,000 service lines under 16 NYCRR 98.1(b). At 50,000 such lines this size exclusion does not apply.
Gas exclusion	Gas corporation that is a SAPA 102(8) small business: resident in NY, independently owned and operated and 100 or fewer employees. Do not substitute SHIELD or DFS size tests.
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	Do not treat an authority or cooperative as municipal by its label. Verify charter, PSL classification, current orders and each actual function. Steam has no matching small-customer exclusion stated in this definition.

Sources: P01, P08, P09.

Applicability: personal information and ownership

Business safeguards and breach law

GBL 899-bb applies to a person or business owning or licensing computerized NY-resident private information. GBL 899-aa defines private information and specifies breach duties for owners/licensees and maintainers. Record where the data subjects reside, who owns/licenses the data and who merely maintains it. New York office location alone is not the complete test.

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 actual governmental function. Its private-information definition, notice wording, ITS consultation and recipient rules need a separate 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 consistent local law. Retrieve that actual instrument. Resolve GBL interaction, operator contracts and records requirements rather than assigning the state-entity process automatically.

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. A qualifying business still needs safeguards appropriate to size, complexity, activities and information sensitivity. A Part 1200 size exclusion does not erase SHIELD, existing PSC orders or contract duties.

Sources: B01, B02, B03, P01.

Data definitions: classify 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. PII alone is not a determination of breach notification.
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 not identical to 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. Do not copy every PSC category into it as if the definitions were identical.
Energy usage	PSL 66(32) makes customer gas/electric consumption confidential. Analyze purpose, consent, tariff and data-access orders even where GBL private-information conditions are not met.

Sources: B01, B03, P01, D01, P07, N02.

The 2013 PII order and current audits

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; do not reset it when starting a new audit.

Nine recommendations

Plan breach response/recovery drills; retain qualified forensic response; arrange credit monitoring; strengthen employee and contractor privacy training; inventory and dispose unnecessary customer information; segregate and mask sensitive information; improve physical protection; strengthen intrusion detection and security-event management; conduct regular third-party vulnerability assessments.

Annual external review

Pages 7-8 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, audit history and current staff instructions instead of assuming a universal January-to-December audit period.

Relationship to Part 1200

The new rule says conflicting existing orders will be abrogated for covered companies as the regulations phase in; existing orders continue for smaller noncovered companies. Build a clause-level transition map. Part 1200.18 adds supply-chain risk, IT/OT segmentation capability and compliance with the Part to its eleven-area yearly third-party audit. Do not discard the legacy plan without determining the actual conflict and phase.

Sources: P03, P01.

Part 1200 transition and recurring calendar

Research cutoff October 16 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 has no transition. 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. This is not a regulator-confirmed business-day-adjusted filing date.
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; seeQ 01.
June 30 yearly from 2027	Prior-calendar-year compliance statement. Support retained five years. Confirm phased-duty representation before signing; seeQ 10.

Sources: P01, P02.

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.
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.

DFS audit timing and filing differences

Recurring review

Subject to actual exemptions, policies have annual approval, risk assessment review/update is at least annual and upon material risk-changing business/technology change, access privileges receive at least annual review, application-security procedures receive annual CISO/designee review, and training includes annual social-engineering awareness. Inventory update/validation frequency follows written procedures. Class A independent audits follow risk assessment, not a frequency invented from PSC rules.

Testing and resilience

Current 500.5 requires at least annual internal/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/BCDR tests and critical-data/system restoration testing. Apply partial exemptions clause by clause and approve safe OT methods separately.

Annual filing

By April 15 submit either a certification of material compliance for the prior calendar year or the specified acknowledgment of noncompliance with affected sections and remediation timeline. Required signers are the highest-ranking executive and CISO, or highest-ranking executive and responsible senior officer if no CISO. Retain support for 5 years. Do not replace this with the PSC June 30 certificate or invent a matching PSC acknowledgment option.

Amendment status

The 2023 second amendment's final two-year transition for MFA and inventory ended November 1 2025. Do not advertise these as future 2026 implementation grace periods for established entities. New status, exemption changes and specific instructions still require entity review.

Sources: D01, D03, D04, D05.

Plan the project and establish authority

Gate 1: scope

PM obtains named entity, systems, period, sponsor, audit lead, data and operating owners. Compliance owner resolves each applicability row or identifies the missing evidence and decision deadline. Audit lead confirms qualifications, independence where required, conflicts and access rights.

Gate 2: readiness

Build evidence request list, controlled exchange route, stakeholder schedule, population/sample plan and method authorization. Confirm site induction, escort, collection devices, no-photography areas, prohibited commands, incident escalation and data-minimization rules. Scope expansion requires approval from the relevant authority.

Gate 3: examination

Collect existing configurations and records, interview owners, perform supervised demonstrations and permitted tests. Keep a daily discrepancy log. Report urgent vulnerabilities and possible incidents immediately through the approved process. Testing stops on abnormal operation, wrong target, lost visibility or unexpected private-data exposure.

Gate 4: decision and closure

Audit lead reconciles findings to criterion and evidence. Sponsor funds/prioritizes action; counsel/compliance resolves legal interpretation and notices; operating owner approves system changes. Independent or separate qualified retest records what changed and the result. PM hands over remaining actions and recurring duties. Proposed duration follows access, scope and testing constraints; no fixed six-week promise is made.

Sources: N01, N03.

Responsibilities and acceptance gates

Role	Accountability and acceptance evidence
Sponsor / governing body	Approves scope, resources and business-risk decisions. Receives material issues and signs only legally appropriate statements based on actual support.
CISO / technical lead	Owns program evidence, risk/control linkage, qualified testing and permitted exceptions. Technical approval states boundary, methods and unresolved limitations.
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 without declaring legal compliance.
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. Challenges unsupported claims, reports limits and verifies corrective actions within approved scope.

Sources: N01, N03, P01, D01.

Evidence request and secure collection

Request package

Request current charter/licenses, PSC entity classification and service-count definitions, historic implementation plan, regulator letters/rubric, last two audits and corrective actions, DFS filings/exemptions, risk assessments, board approvals, asset/application/vendor lists, customer-data flows, policies, access reviews, test reports, incident logs, exercise/restoration results, contracts and retention schedule. Specify period, owner, delivery date and acceptable redactions.

Evidence record

Assign an evidence ID. Record system/control, custodian, source record/period, extraction method and filters, collection timestamp and timezone, integrity value where useful, access restrictions, controlled location, retention/hold and linked sample IDs. Preserve original time data and explain any normalized display. Record who supplied a statement separately from who observed a result.

Minimum necessary

Use aggregate counts, synthetic customer records, redacted screenshots and supervised displays where sufficient. Do not place raw customer names, SSNs, bank credentials, passwords, tokens, topology or live vulnerabilities in website fields or ordinary spreadsheets. The workbook stores controlled references. Agree a secure evidence repository before collection.

Regulator disclosure

Part 1200 confidentiality is subject to applicable disclosure exemptions; it is not an automatic blanket secrecy guarantee. Follow actual filing procedures for restricted material and involve the records/FOIL decision maker. Do not assert attorney-client privilege merely because the pack is used by legal staff.

Sources: P01, D01, N01, N02.

Sampling and assessment conclusions

Define populations

For each test record complete population, period and source. Examples include all privileged users across scoped systems, terminated workers in period, active suppliers handling NPI, external customer-data transfers, critical recovery services and known exceptions. Reconcile source totals before selecting samples.

Select deliberately

For proposed judgmental sampling, examine high-consequence systems, emergency accounts, exceptions, material changes and prior failures, then representative ordinary records. State counts and selection reasons. If using statistical sampling, obtain qualified design and document confidence, precision and limitations separately. No sample size is mandated by this generic pack.

Expand on failure

A missing MFA policy is a design issue; an approved policy with an unprotected direct login is an operating failure. Expand to related systems/users/providers when a failure could be systemic. Escalate evidence gaps and scope restrictions. A vendor assurance report must match the service, period, tests and applicable customer responsibilities.

Use precise result states

Record Not examined, Evidence requested, Supported, Exception found or Not applicable with basis. A supplied narrative is not a successful test. Record the condition, criterion, evidence, sample extent and test limitations. No finding does not prove full compliance when populations or tests are incomplete.

Sources: N01.

Field procedure: billing, AMI and access

Before arriving

Confirm target systems, safe read-only collection method, escort, expected baseline, approved synthetic identities and account roles. Check whether the meter platform or historian interface can affect physical operations. Obtain explicit additional authority for any live authentication, export or connectivity demonstration.

Observe and record

Reconcile billing/MDM/AMI inventory identifiers to approved diagrams. Ask the owner to show synthetic customer search, role masking, export authorization, consent enforcement and audit event capture. Record method, time, user role, expected/actual outcome and evidence reference. Compare joiner/leaver and vendor access samples with approval and revocation records.

Protect operations

Do not alter meter configuration, issue disconnect commands, enumerate controllers, replay traffic or conduct vulnerability probes under a document-review work order. Check relevant DNP3, Modbus, IEC61850 or proprietary interface paths from engineering evidence where present; a protocol name is not evidence of vulnerability or authorization to test.

Stop and hand back

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

Sources: N03, P01.

Field procedure: segmentation and recovery

Trace dependencies first

Map 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. Obtain the actual operating owner's acceptance of the method and sequence.

Assess without live disruption

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

Verify service recovery

Inspect evidence that required identity, keys, application dependencies, data and supplier services can be restored in the necessary sequence. A successful backup job is not restoration proof. Distinguish tabletop, lab restoration, partial component test and full service recovery. Record actual measured results rather than promised recovery objectives.

Exception handling

A technical safety constraint requires a documented alternate method and compliance decision. It does not automatically excuse a mandatory testing duty. Carry untested paths and unresolved legal acceptance into findings and the adoption record.

Sources: N03, P01, D01.

Notification clocks: keep triggers 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 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. No imported universal 30-day cap.

Sources: P01, D01, B01, B03.

Incident threshold screen and escalation

PSC event and incident

Part 1200 defines events broadly, including unsuccessful access/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/supervisory notice duty. Apply the full 1200.1(d)-(e) wording. Maintain the event/incident log even for events not subject to the 72-hour notice.

DFS incident

Part 500.1(g) concerns events at the entity, affiliate or TPSP that impact the covered entity and require notice to a government/self-regulatory/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. Keep each determination, 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 rather than suppressing access-only evidence or assuming the definitions are identical.

Immediate internal action

A technician or analyst records the observed facts and notifies the designated incident authority promptly. Preserve evidence, protect service and follow approved containment. Legal/compliance evaluates parallel duties without waiting for every affected record or the final investigation report. If a trigger is uncertain, record uncertainty and the next decision owner/time; do not treat uncertainty as a legal pause.

Sources: P01, D01, B01, B03.

Resident notices and regulator coordination

GBL recipients and content

When NY residents are notified, notify AG, Department of State and State Police as to timing, content, distribution and approximate affected count; include the notice template without delaying resident notice. The statute additionally addresses DFS notice for DFS-covered entities pursuant to 500.17. More than 5,000 NY residents notified at one time triggers consumer reporting agency notice. Review required notice contact details, data categories and permitted delivery method.

State route and local procedure

STL 208 uses AG, 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 after notice, not permission for an operator to wait 90 days to notify. Local agencies must retrieve their adopted policy/law and escalation route.

Exceptions and alternative notices

Use the precise inadvertent-authorized-disclosure/harm conditions. Keep the written determination 5 years; if over 500 NY residents are affected, provide it to AG within 10 days of determination. Qualifying notice under another specified regime may avoid duplicate resident notice but does not eliminate remaining agency/CRA duties. HIPAA/HITECH-related AG notice provisions require separate assessment, including the 5-business-day rule after HHS notice.

Execution

Verify current authenticated channels before an incident. Record approver, facts known/unknown, legal basis, timestamps, submitted version, receipt, updates and delivery exceptions. Do not delay a triggered report for a perfect root-cause analysis. Contracts may require earlier supplier or insurer notice. The workbook creates a decision record, not a filed notice.

Sources: B01, B03, B04, D01, P01.

Data access, consent and supplier agreements

Scope the transaction

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

Test a controlled disclosure

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

Aggregation

Do not assume removal of names makes interval consumption anonymous. Determine the current use-case-specific aggregation screen and later PSC clarifications, approved data recipient and re-identification controls. This pack deliberately does not supply a universal numeric threshold. Q07 requires the current operative tariff/order set before release.

Contract examination

Check required safeguards, remote/privileged access, incident notification, subcontractors, audit/evidence access, retention, return/destruction, legal holds and termination. A SOC report is evidence within its scope and period; it does not automatically satisfy a utility's full regulatory audit or a recipient's contractual duties.

Sources: P04, P05, P06, P07, D06.

Report, remediate and hand over

Report structure

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

Correction process

Agree each finding's factual accuracy without allowing an evidence-based result to be removed for preference. Assign accountable owner, target date, dependencies, resources and interim controls. Record mandatory deadline separately from proposed project target. Document rejected recommendations and 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 only when the criterion, evidence and verification decision support closure. Reopened failures and changed scope retain history.

Handover

PM confirms recipient access to retained records, named owners of all open questions/actions, current notification contacts, recurring calendar and transition decisions. Obtain technical, compliance and operating acceptance with scope/date. Personal owner review or legal sign-off is established only by an actual completed record.

Sources: N01, P01, D01.

Control procedures C01 to C02

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: No blanket determination based on sector or ownership. Missing facts stay 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: No statistical assurance or organization-wide pass inferred from a judgmental sample. Owner: Audit lead.

Sources: P01, D01, B02, B03, N01.

Control procedures C03 to C04

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. Unmapped copies remain open. 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; no assumed safe harbor from registration alone. Owner: CISO.

Sources: B01, B02, N02, P01.

Control procedures C05 to C06

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 without opening live cabinets or copying personal data.

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.

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, not a stopped clock. Owner: Incident commander.

Sources: B02, N02, N03, B01, B03, D01, P01.

Control procedures C07 to C08

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 do not become universal deletion dates. P01 1200.13 cross-reference unresolved. 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 is not Verified. Mandatory duties cannot be waived by a management risk-acceptance entry. Owner: Audit lead.

Sources: B01, B02, D01, P01, N01.

Control procedures P01 to P02

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.

Control procedures P03 to P04

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: Do not import the old DFS continuous-monitoring alternative into current DFS 500.5. No OT test authorized by this review. 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.

Request: Path diagram, role-to-field map, masking policy and test evidence. Acceptance: Document accessible data and bypasses. A VLAN drawing alone does not prove isolation or masking. Owner: Technical lead.

Sources: P01, N03.

Control procedures P05 to P06

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. A completion percentage does not establish comprehension or control effectiveness. 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, P03.

Control procedures P07 to P08

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 have evidence and scope, not an assumed exemption. Owner: Facilities owner.

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. No claim that backups restore service without restoration evidence. Owner: Recovery owner.

Sources: P01.

Control procedures P09 to P10

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 alone is insufficient. 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: No live disconnection or active OT scan under document review authority. Record untested paths and service consequences. Owner: OT operating owner.

Sources: P01, N03.

Control procedures P11 to P12

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. Acceptance: The eleven audit areas do not replace a full rule mapping. No certification generated from a checklist score. 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 not represented as proof of completed investigation. Duty subject to transition and actual incident facts. Owner: Incident commander.

Sources: P01, P02, B01.

Control procedures D01 to D02

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: No exemption inferred from utility ownership or a checked box. 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.

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, D02, D03, D07.

Control procedures D03 to D04

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: Missing systems and unsupported residual-risk conclusions remain visible. 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: Continuous monitoring alone is not substituted for current DFS annual penetration duty. Unsafe OT gaps escalated for a compliant approved method. Owner: Technical lead.

Sources: D01, D05, N03.

Control procedures D05 to D06

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.

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 using current DFS FAQ, not a blanket login mandate. 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: Do not invent annual Class A audit frequency from the PSC yearly audit or claim every exception applies to every control. Owner: Audit lead.

Sources: D01, D04, D03.

Control procedures D07 to D08

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: Outsourcing does not transfer accountability. Guidance recommendations not promoted to new regulations. 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: No general transit-encryption exception copied from PSC. Retention minima applied to defined record classes. Owner: Technical lead.

Sources: D01, D06, D07.

Control procedures D09 to B01

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. No automatic certification. 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: Do not claim all utility PII triggers GBL notice or apply GBL additions wholesale to STL. Owner: Privacy lead.

Sources: D01, B01, B03, P01, P07.

Control procedures B02 to B03

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: Do not wait for full forensics or treat 30 days as permission to delay. 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.

Request: Charter analysis, adopted local policy, state consultation records and recipient matrix. Acceptance: No automatic state-entity classification for municipal ownership. No fabricated universal municipal 30-day clock. Owner: Compliance owner.

Sources: B01, B04, B03.

Control procedures B04 to B05

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. No blanket HIPAA or DFS waiver of all NY notifications. 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: Do not claim a universal aggregation safe harbor or apply energy-market rules to all water-sector exchanges. Owner: Privacy lead.

Sources: B01, B03, P04, P05, P06, P07.

Control procedures B06 to B06

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 not copied into public workbook. No medical category assumed to make the whole utility HIPAA-covered. Owner: Privacy lead.

Sources: B01, B02, N02.

Additional control procedures P13 to P14

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 remain uncompleted.

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. A generic score is insufficient. Proposed owner: Risk manager. Actual results and reviewer remain uncompleted.

Sources: P01.

Additional control procedures P15 to P16

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 remain uncompleted.

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 are not copied into DFS transit-encryption requirements. Proposed owner: Technical lead. Actual results and reviewer remain uncompleted.

Sources: P01.

Additional control procedures D10 to D11

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 remain uncompleted.

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 without exposing secrets.

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

Conclusion boundary: No filing or exemption inferred from generating this workbook. Proposed owner: Compliance owner. Actual results and reviewer remain uncompleted.

Sources: D01.

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.

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.

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.

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.

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.

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 and instrument status

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 adopted definitions rather than simplified customer-count summaries. Apparent cross-reference errors and first-year scheduling require 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. Cover states it is not the official version. Reconcile the operative codified text and later amendments before a signed legal conclusion.

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. Different 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 tailored safeguards, not no safeguards.

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. Do not import GBL clock or definition wholesale.

Sources: P01, D01, B01, B02, B03.

Sources and instrument status

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, not automatic NY legal compliance or a mandatory universal control baseline.

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. Does not impose an independent new universal utility duty.

D02 Cybersecurity resource center

NYS Department of Financial Services. Agency guidance and current resource index. Covered entities, regulation and submissions links. Utility status alone is not DFS coverage. Guidance does not amend a regulation.

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, N03, D05, D02, D03.

Sources and instrument status

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 actual legal entity and function, not marketing sector labels.

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. Different from DFS and SHIELD 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. Does not make every utility subject to NERC CIP or Part 500.

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. Its PII concept does not replace NY statutory private-information definitions.

Sources: D07, P08, P09, P07, N02.

Sources and instrument status

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 differ.

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 not assumed to require customer MFA.

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; a single portal does not prove every notice was delivered.

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; not a universal rule for all utility vendors. Check later amendments and the executed agreement.

Sources: P03, P02, D04, B04, P04.

Sources and instrument status

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 must be checked against later orders, the actual use case and current tariff.

P06 Data Access Framework clarification

NYS Public Service Commission. Final order. Case 20-M-0082, November 18 2021, clarification and tariff modifications. Do not use the initial framework without subsequent clarification and applicable tariff.

D06 Third-party service provider risk guidance

NYS Department of Financial Services. Agency guidance. October 21 2025; selection through termination. Expressly does not impose new obligations. Distinguish recommendations from Part 500 mandates.

Sources: P05, P06, D06.