Content review findings and unresolved authority

Planning edition October 15, 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.

3 Review scope and unresolved authority
4 Review findings 1 to 3
5 Review findings 4 to 6
6 Review findings 7 to 9
7 Review findings 10 to 12
8 Review findings 13 to 15
9 Review findings 16 to 17
10 Unresolved questions Q01 onward
11 Unresolved questions Q03 onward
12 Unresolved questions Q05 onward
13 Unresolved questions Q07 onward
14 Unresolved questions Q09 onward
15 Sources and instrument status
16 Sources and instrument status

Review scope and unresolved authority

Review method

The content review challenged applicability, thresholds, date triggers, legal-versus-guidance status, entity boundaries and evidence sufficiency. The usability review followed sponsor, project-manager and field-technician workflows, including unknown facts, no-JavaScript access, local generation, error recovery and safe defaults. Accuracy checks compared statements to the cited primary instruments.

Scope of assurance

This report records editorial and technical content review of the planning edition. It is not a regulator examination, legal opinion, independent external audit or evidence of an actual utility's compliance. No personal technical review by Joseph Caruso or other named person is asserted without their completed adoption record.

Material unresolved items

Q01-Q10 identify first-year timing, apparent drafting discrepancies, confidential/entity-specific criteria and ownership/instrument decisions. Use them as project tasks with an owner and required resolution evidence. No open item is silently converted to a conclusion.

Sources: P01, P03, D01, B01, B03, N01.

Review findings 1 to 3

R01 Accuracy Utility equals DFS covered entity

Disposition: Refuted. Coverage gate tied to qualifying authorization under Banking, Insurance or Financial Services Law. Shared systems separately mapped.

Basis: D01 500.1(e); D02.

R02 Accuracy Part 1200 is still proposed

Disposition: Refuted. Final April 2026 adopted text and May adoption notice used, with June 1 effective date. Draft January 2026 effective date rejected.

Basis: P01; P02.

R03 Accuracy Every water electric utility with 50 000 customers is covered

Disposition: Refuted. Exact water fewer than 50,001 service connections and electric fewer than 50,000 service lines exclusions retained. Ownership and legal entity still checked.

Basis: P01 1200.1(c).

Review findings 4 to 6

R04 Adversarial A privacy audit authorizes live OT isolation or scans

Disposition: Refuted. Document-first assessment and separate operating permit. Rule IT definition excludes OT; segmentation capability reviewed safely. DFS scope separately evaluated.

Basis: P01 1200.1(g),(r); D01 500.1(i); N03.

R05 Accuracy Continuous monitoring substitutes for DFS annual penetration test

Disposition: Refuted. PSC conditional alternative separated from current DFS 500.5 requirements.

Basis: P01 1200.5; D01 500.5.

R06 Accuracy Annual audit and risk assessment intervals are interchangeable

Disposition: Refuted. PSC yearly third-party audit, biennial risk assessment, DFS annual risk review and risk-based Class A independent audit distinguished.

Basis: P01 1200.9,1200.18; D01 500.2(c),500.9.

Review findings 7 to 9

R07 Accuracy NY breach law only covers acquisition and has no fixed outer limit

Disposition: Refuted. Current GBL access-or-acquisition definition, medical/health additions and 30-day limit retained. STL treated separately.

Basis: B01; B03.

R08 Accuracy Municipal utilities are state entities under STL 208

Disposition: Refuted. Explicit exclusion and local notification-policy duty both included. GBL interaction left entity-specific.

Basis: B03 1(c),10.

R09 Adversarial SHIELD small business has no safeguards duty

Disposition: Refuted. Tailored safeguards required. DFS, SAPA and SHIELD size tests not mixed.

Basis: B02; P09; D01.

Review findings 10 to 12

R10 Adversarial A NIST mapping or partial DFS exemption proves compliance

Disposition: Refuted. Clause decisions, evidence, exemptions and risk decisions separate. No numerical compliance score or automatic certification.

Basis: B02; D01; N01.

R11 Usability Unresolved choices can disappear from a customized set

Disposition: Corrected. All applicability records, source register and open questions retained. Selected modules tailor detailed work only. Coverage decisions stay Unresolved.

Basis: Builder and workbook design.

R12 Usability Field technicians must collect raw customer data to prove controls

Disposition: Corrected. Synthetic records, supervised displays and secure evidence references specified. No uploads or customer data in public builder.

Basis: N02; N03.

Review findings 13 to 15

R13 Accuracy 2013 order creates new 60 day deadline for every new audit

Disposition: Refuted. Original implementation-plan deadline identified as historical. Current plan, audit anniversary and staff directions must be retrieved.

Basis: P03 pages 7-9.

R14 Accuracy PSC forensic credit monitoring contracts are optional suggestions forever

Disposition: Refuted. Final Part 1200.19-.20 duties and general transition included; qualified forensic supplier and at least one-year credit offer conditions preserved.

Basis: P01 1200.19-.20,.25.

R15 Accuracy Correct obvious legal drafting errors silently

Disposition: Sustained - open. Cross-reference/form/wording discrepancies listed Q02-Q04. No invented correction or assurance of official filing acceptance.

Basis: P01.

Review findings 16 to 17

R16 Adversarial Audit package establishes professional legal approval or personal owner review

Disposition: Refuted. Blank adoption fields. No signature, personal technical review, legal advice engagement or regulatory approval asserted.

Basis: Pack adoption and evidence rules.

R17 Accuracy First year September audit and certification timing are fully settled

Disposition: Sustained - open. Q01 and Q10 require written DPS clarification. Phase-in intervals preserved rather than fabricated filing dates.

Basis: P01 1200.18,.21,.24-.25.

Unresolved questions Q01 onward

Q01 PSC first audit date

1200.18(c) says September 15 yearly while 1200.25 gives a general 180-day transition. September 15 2026 precedes that interval. Confirm first required availability date and legacy PII audit continuity with DPS.

Owner: Compliance owner. Basis: P01 1200.18(c),1200.25; P03. Required resolution: Written DPS direction and entity audit history.

Q02 Retention cross reference

Adopted 1200.13 refers to 1200.1(i)(2)-(4), although NPI is defined in 1200.1(j) and (i) defines MFA. Do not silently repair the legal text.

Owner: Legal lead. Basis: P01 Appendix A page 10. Required resolution: Current codified text, errata or written regulator clarification.

Sources: P01, P03.

Unresolved questions Q03 onward

Q03 Exemption form cross reference

Appendix 19 cites 1200.21(a) for exemption, while the exemption provision is 1200.23(a). Verify current form and filing instructions before use.

Owner: Compliance owner. Basis: P01 Appendix 19 and 1200.23. Required resolution: Current official exemption form and accepted channel.

Q04 Incident provision wording

1200.21(a) contains the phrase on public information in the adopted attachment. Clarify against current filed/codified text; use broad escalation for suspected NPI incidents meanwhile.

Owner: Legal lead. Basis: P01 Appendix A page 14. Required resolution: Corrected or controlling text and written response.

Sources: P01.

Unresolved questions Q05 onward

Q05 Utility specific DPS rubric

Public rules describe staff rubrics, but a current complete entity-specific DPS PII Implementation Plan Review Worksheet and correspondence were not established in this research. This pack is not that official rubric.

Owner: Audit lead. Basis: P01 1200.17; P03. Required resolution: Authorized current staff request list/rubric and utility implementation plan.

Q06 Ownership and jurisdiction

Municipality, cooperative, public authority and public benefit corporation labels do not settle every definition. Determine charter, PSC jurisdiction, operating contractor role and local notification policy.

Owner: Compliance owner. Basis: P01 1200.1(c); B03 1(c),10. Required resolution: Charter and signed entity-specific legal analysis.

Sources: P01, P03, B03.

Unresolved questions Q07 onward

Q07 Data access instruments

Current utility tariff, DSA/self-attestation, later PSC orders, data access purpose and customer authorizations must be retrieved. No universal aggregation threshold or approved vendor status is certified here.

Owner: Privacy lead. Basis: P04-P07. Required resolution: Current effective instruments and executed agreement.

Q08 DFS operative baseline

DFS-hosted reading copy labels itself unofficial. Reconcile codified Part 500, amendments and the entity license/exemption record before a signed determination. Older guidance uses old subsection numbers.

Owner: Compliance owner. Basis: D01-D07. Required resolution: Current controlling version plus license and exemption evidence.

Sources: P01, D01, P04.

Unresolved questions Q09 onward

Q09 Other jurisdiction and incident duties

Entity-specific NERC CIP, TSA, SEC, drinking water, wastewater permit, state/local procurement and insurer/contract duties are outside a universal NY privacy conclusion. Assign separate screening owners.

Owner: Compliance owner. Basis: P07; N03. Required resolution: Applicable current instruments, confidential directions and responsible officials.

Q10 First certification scope

June 30 2027 certification covers the prior year while several requirements have later transitions. Confirm treatment of phased duties and current form instructions with DPS before signing.

Owner: CISO. Basis: P01 1200.21(c),1200.24-1200.25. Required resolution: Written interpretation and clause-by-clause support for applicable period.

Sources: P01.

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.

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.

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.

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, P03, D01, B01, 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.

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: N01, P04.