

New York power and energy cyber audit preparation

Determine the entity and asset boundaries before combining utility IT records, operational systems and electricity-sector requirements. A distribution system, DER operator, generator and BES-related entity do not automatically have the same obligations.

Scope first. PSC adopted 16 NYCRR Part 1200 in Case 25-M-0302. Its definitions, exclusions and phase-in provisions matter. Utility IT requirements and applicable NERC CIP obligations are different scopes; neither is a universal requirement for every power or energy organization.

Review period: _____ Responsible role: _____

Item	Records and next decisions	Working status
PE-01	Entity and authority map Record the entity, PSC status, registrations, contracts and responsible compliance owner. Next: Resolve covered-entity definitions, exclusions and applicable versions before choosing requirements. Source: PSC1; NERC1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
PE-02	IT, OT and BES scope Prepare a controlled asset/function map distinguishing business IT, plant OT and any applicable BES scope. Next: Do not apply NERC CIP to all distribution/DER assets or treat IT rules as an OT standard. Source: PSC1; DOE1; NERC1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
PE-03	Risk and consequence record Gather risk assessments and dependencies affecting service, safety, customer information and recovery. Next: Prioritize with operations and compliance rather than ranking by office-IT severity alone. Source: PSC1; DOE1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
PE-04	Access and third-party paths Gather identity records, vendor pathways, approvals and privileged-access settings. Next: Have owners reconcile who can reach each relevant environment. Source: PSC1; DOE1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
PE-05	Asset and change evidence Reconcile configuration, software, network and engineering change records. Next: Record missing owners and baseline differences before selecting a review sample. Source: DOE1; NERC1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*

Statuses are self-reported and unverified. Gathered means a record was located, not that a control passed. *Document the basis for any not-applicable choice in the editable CSV.

CONTINUE / EVIDENCE AND OPEN DECISIONS

Item	Records and next decisions	Working status
PE-06	Logs and time correlation Gather source coverage, retention, time settings and event export methods. Next: Identify gaps that limit incident reconstruction without moving sensitive operational data to a public tool. Source: PSC1; NERC1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
PE-07	Safe validation plan Document authorized methods, device constraints, test windows, stops and recovery contacts. Next: Use passive records or controlled replicas first; active production work needs operator approval. Source: DOE1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
PE-08	Corrective work and verification Gather issue ownership, risk decisions, tickets, exceptions and retest records. Next: Trace each claimed correction to an observable result. Source: PSC1; DOE1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
PE-09	Response and restoration exercise Gather response plans, backup/restore evidence, escalation and exercise lessons. Next: Verify operating dependencies with the designated authority before declaring a recovery path usable. Source: PSC1; DOE1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
PE-10	Review package and remaining questions Index source versions, covered populations, findings and unresolved authority decisions. Next: Keep consultant workpapers separate from regulator or Regional Entity determinations and filings. Source: PSC1; NERC1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*

Finish the preparation record

In the companion CSV, record an owner, evidence reference and open question for each item. Keep actual files in your approved repository. Ask the responsible technical, compliance and legal teams to resolve scope, phase-in dates and signatory authority. This worksheet performs no audit, scan, filing or legal determination.

Official sources

PSC1 - PSC adopted utility IT cybersecurity regulations, Case 25-M-0302, April 17, 2026

DOE1 - DOE cybersecurity baselines for electric distribution systems and DER

NERC1 - NERC Critical Infrastructure Protection standards

Discuss technical scope: newyorkcomputerforensics.com/contact/ | 212-561-5860. Do not send operational records or evidence through the public form.