Power and energy OT assessment planning pack

Planning edition October 16, 2026

Operational technology, industrial control systems and supervisory control and data acquisition

United States federal requirements with a 50-state and local applicability companion

Purpose

Plan the work, establish the applicable obligations, collect traceable evidence, protect operating authority and carry corrective actions through verification and handover.

Working records

Use the editable project workbook for applicability, work planning, evidence, findings, local duties and notification decisions. Fillable worksheets are included in the sector manuals and state/local companion. Save completed records only in the approved location.

Facility adoption

Complete the site-specific decisions and obtain the responsible operating, technical and compliance approvals. Unresolved instruments and local requirements are listed in the review report. The research edition does not contain a facility compliance determination.

Contents

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

3 Planning scope and research basis
4 Using the corrected workbook edition
5 Using this planning pack
6 Decisions before mobilization
7 Roles and decision authority
8 Project stages and acceptance
9 Applicability and obligation records
10 Bulk power applicability
11 CIP evidence workstreams
12 Distribution DER and state utility programs
13 Substation and control center examination
14 Power incident and recovery exercise
15 Power reporting and recurring calendar
16 Document requests and interviews
17 Safe work and stop authority
18 Inventory and process dependencies
19 Network paths and remote access
20 Accounts legacy systems and suppliers
21 Monitoring time and evidence handling
22 Recovery and continuity evidence
23 Authorization for active validation
24 Writing findings that can be audited
25 Corrective work and management reporting
26 Verification closure and recurring work
27 Facility and applicability worksheet
28 Field activity authorization worksheet
29 Evidence and finding worksheet
30 Corrective action and acceptance worksheet
31 Terms used in the planning records
32 Sources and instrument status
33 Sources and instrument status
34 Sources and instrument status
35 Sources and instrument status
36 Sources and instrument status

Planning scope and research basis

This pack supports a controlled assessment of generation, transmission, distribution, protection, dispatch, storage, gas operations and supporting station services in the United States. Use the companion volume to screen all 50 states and resolve the actual local and facility requirements.

What the assessment produces

An approved scope, applicability register, process dependency map, examined evidence, safe activity records, consequence-based findings, corrective plan and verification record. The workbook and fillable worksheets carry the work from planning through handover.

Research cutoff

The regulatory research cutoff is October 16, 2026. Current public primary sources, official program material and selected peer reviewed research support the text. Effective instruments take precedence over guidance and this planning edition. Full normative ISA/IEC standards, operator security directives, facility permits and private contracts were not supplied.

Open applicability

The source register marks restricted retrieval, older or expired instruments, drafts and unresolved questions. A 50-state screening is not an exhaustive legal opinion on every locality. Use the identified gaps to obtain the controlling text and facility facts before signing a site-specific conclusion.

Adoption and review

Complete the facility-specific records and obtain the named operating, technical and compliance approvals. The recorded adversarial content, usability and accuracy reviews are in the Review findings and unresolved questions report.

Sources: F01, F02, R01, R02, R03.

Using the corrected workbook edition

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

Before execution

Use the exact criterion, population, period, sampling rationale, permitted method, execution date, actual observation, evidence IDs and reviewer. A proposed test is not an assessment result. Keep sources and operating authority separate.

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, its reason and responsible reviewer in Scope decisions. Deferred work remains visible. State research is a separately labelled routing register; the 200 state-sector rows are research tasks. For NY use the Clause matrix and Q01-Q10. Missing current instruments and local facts remain unresolved.

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: F01, F03.

Using this planning pack

Use this pack to organize an assessment of generation, transmission, distribution, protection, dispatch, storage, gas operations and supporting station services. Start with the legal and operating boundary. Select evidence and methods only after the people responsible for the process agree what may be examined.

First use

Read the sector applicability pages, then the State and local applicability companion. Create one record for each legal entity, facility and regulatory program. The workbook contains 200 open state-sector research rows and a separate 50-note selected-source register. Those rows are research prompts, not completed facility determinations.

Appoint a sponsor, operating owner, technical lead, compliance owner and project manager. Complete the site worksheet. Resolve mandatory instruments and operating permissions before scheduling intrusive work. Use the field authorization sheet for each approved activity.

Reading the evidence

The pack separates binding law or an incorporated instrument, agency guidance, standards, and proposed assessment procedures. A citation identifies the source for a regulatory statement. Procedure descriptions explain how the assessment team can collect evidence; they do not create a new legal obligation.

A rule can be effective while a particular requirement has a later compliance date. An approved standard can still be subject to future enforcement. Record both dates and the applicable version. Never infer a deadline solely from a publication date.

Before signing an assessment conclusion

The reviewer needs the actual facility facts, current instruments, examined evidence, test permissions and unresolved limitations. No facility has been assessed by preparing this pack. A named technical reviewer must review the completed work before the organization adopts or publishes its conclusions.

Sources: F01, F03.

Decisions before mobilization

Separate registered bulk-power functions and BES Cyber Systems from distribution-only systems, DER, gas facilities, pipelines and nuclear licensed systems. A common corporate owner does not give these systems identical obligations.

Define the work product

Decide whether the engagement is an engineering risk assessment, a gap assessment against named requirements, independent assurance, or a combination with separated responsibilities. Name the intended recipients and who may receive the technical appendices. If the team designed the controls, disclose that relationship before describing its work as independent.

Record the facility boundary

Identify EMS and DMS platforms, substation gateways, relays, RTUs, plant DCS, engineering stations, historians, DER controllers and vendor remote access. Include supporting identity, DNS, time, virtualization, telecommunications and backup dependencies when their failure could affect the process. Identify shared corporate services and third-party interfaces without silently expanding test permission.

Record legal entity, physical address, owner, operator, sector, production or service function, permits, regulators, contracts, insurer conditions and public-body status. For distributed assets, list the other states, local authorities and control centers involved.

Define exclusions

Document excluded safety systems, inaccessible vendor appliances, unsupported firmware, unapproved protocols and unavailable evidence. State how each exclusion limits the conclusion. An excluded critical dependency must remain visible to the sponsor rather than disappearing from the asset count.

Release decision

The sponsor approves purpose and resources. The operating owner approves the process boundary. The compliance owner signs the applicability register. The technical lead signs the method. The project manager records the dependencies and unresolved items. Silence is not approval.

Sources: F01, F03.

Roles and decision authority

Assign people and alternates before work starts. Small organizations may combine roles, but operating authorization, evidence review and risk acceptance must remain explicit.

Role	Decision or work owned
Sponsor or CISO	Approves business objective, resources and reporting audience. Accepts residual business risk only within delegated authority.
Operating owner and engineering authority	Approve process boundaries, safe state and production methods. The control center and responsible electrical authority retain switching, dispatch and protection authority. Do not alter relay settings, issue switching commands, trip equipment or test failover in a live grid without an approved operating procedure.
Compliance owner and counsel	Resolve applicable instruments, disclosure restrictions and incident-reporting duties. Identify the responsible filing official and alternate.
Technical lead and field technician	Design the permitted method and collect traceable evidence. A technician cannot expand the target list or authorize an active test.
Project manager	Sequences work, tracks evidence and approvals, protects operating windows, manages changes and closes acceptance records.
Evidence custodian and quality reviewer	Control evidence access, integrity, retention and independent review of facts and conclusions. Record conflicts and review exceptions.

Sources: F01, F03.

Project stages and acceptance

Plan by completed decisions and evidence, rather than a fixed number of days. Populate durations and staffing only after site access, document availability and maintenance windows are known.

Stage	Required exit evidence
1 Applicability and scope	Signed facility register, controlling instruments, exclusions and reporting scope. Open legal questions have an owner and defined effect on the engagement.
2 Readiness	Approved evidence request, interviews, collection method, secure workspace, current backup evidence and operating contacts.
3 Examination	Asset and process records, reconciled diagrams, sampled control evidence and a dated account of what was examined.
4 Authorized validation	Activity permits, baseline observations, test log, stop/recovery record and post-work operating acceptance. If validation was not authorized, record that limit.
5 Reporting and decisions	Reviewed findings, requirement mappings, limitations, corrective owners, funding decisions and a residual-risk record.
6 Verification and handover	Retest evidence, recurring review schedule, retained records, lessons and signed handover. Recommendations remain open until verified or formally dispositioned.

Sources: F03.

Applicability and obligation records

Use one row per obligation. A facility can have several reporting clocks, evidence packages and responsible officials for the same event.

Make a defensible decision

For each candidate instrument, record the issuing authority, legal citation, adopted version, effective date, compliance date, regulated entity, covered system, trigger and exceptions. Link the source copy and the evidence establishing the facility facts. Mark the site decision Applicable, Not applicable with reason, or Unresolved.

Do not mark an item Not applicable because no search result was found. Lack of a public directive, missing permit or restricted document creates an information gap. Determine whether that gap prevents a compliance conclusion, a test activity, or only a future work item.

Separate obligation types

Federal requirements, state utility orders, public-agency standards, local permits and contracts can overlap. Guidance and a draft standard remain advisory unless a controlling instrument incorporates them. An insurance condition is a contractual requirement, not automatically a law.

Use the 50-state companion to select additional checks. Confirm municipality, county, tribal or territorial authority where relevant. Municipal ownership can change utility jurisdiction and public-entity duties. It does not remove federal obligations that independently apply.

Preserve the reasoning

The compliance owner signs the decision date and next review trigger. Save the instrument and its source URL in controlled records. Record who will check amendments. For an incident clock, record the trigger event, start timestamp and timezone, deadline rule, recipient, permitted channel, responsible official and receipt.

Sources: F01, F05, F09.

Bulk power applicability

NERC CIP applicability begins with the registered function, facilities, systems and applicable standard. It does not follow from the word energy in a company description.

Freeze the applicability record

Obtain the entity registration, functional roles, relevant facilities, BES Cyber System categorization, asset ownership and accountable compliance owner. Identify applicable exceptions and system boundaries. Record the exact requirement and version rather than a generic CIP compliant label.

Separate current and future enforcement

The NERC register distinguishes mandatory standards from standards subject to future enforcement. FERC approved further virtualization and low-impact changes in March 2026. Keep the order, implementation plan, enforcement date and transitional scope together. Do not assume that a newly approved revision replaces the enforceable edition on the approval date.

Other energy boundaries

Distribution-only systems, DER, gas operations and pipelines need separate state, contractual and federal reviews. Nuclear licensee cyber programs under 10 CFR 73.54 have their own authority and approved plan. Resolve overlaps at the specific system boundary with the responsible compliance owners.

Evidence accepted

The compliance owner signs the registration, categorization and requirement matrix. Include a controlled copy of each applicable instrument and a future-change watchlist. Any missing current standard or unresolved boundary prevents a complete CIP compliance conclusion for that item.

Sources: P01, P02, P03, P05.

CIP evidence workstreams

Use these as candidate evidence workstreams. Each row requires the applicable requirement, edition, system and population to be established first.

Workstream	Evidence and examination
Categorization and governance	CIP-002 and CIP-003. Review categorization rationale, responsible roles, policy approval and the applicable low-impact controls. Do not apply high/medium-impact testing indiscriminately to low-impact scope.
People and electronic access	CIP-004 and CIP-005 where applicable. Examine authorization, training, remote access, electronic boundaries and revocation samples. Keep the exact population and assessment period.
Physical and system controls	CIP-006 and CIP-007 where applicable. Review access records, approved system-security processes and evidence of operation. Identify legacy limitations and required exceptions.
Incident and recovery plans	CIP-008 and CIP-009 where applicable. Review the plan version, exercise or test evidence, roles, results and corrective work. An ERP paragraph does not prove a completed technical recovery test.
Configuration and vulnerability work	CIP-010 where applicable. Link baseline, change and assessment evidence to the named system and requirement. Do not assume a generic vulnerability scan satisfies every required method.
Information supplier and future monitoring scope	CIP-011, CIP-013 and other applicable standards. Review protected information and supplier-risk evidence. Track CIP-015 and other future obligations separately until their exact enforcement and system scope are confirmed.

Sources: P01, P03.

Distribution DER and state utility programs

State oversight, public-power governance and contracts can matter when NERC CIP does not apply to the scoped system.

Determine the operator

Record investor-owned, municipal, cooperative, independent generator, storage or aggregator status. Identify commission jurisdiction, public-body rules, interconnection arrangements, tariffs, operational agreements and any state-specific cybersecurity instruments.

Use the actual state instrument

New York's April 2026 PSC announcement describes utility IT rules effective June 1 2026 and distinguishes future OT rulemaking. Do not relabel those IT rules as a complete OT assessment mandate. Delaware describes annual Class A utility cyber filings. Tennessee and other states have separate utility programs that need current scope and filing checks.

Use guidance appropriately

The NARUC and DOE distribution baselines can support a gap assessment when agreed by the owner. They are not a nationwide binding distribution regulation. Identify any commission order or contract that adopts them and use the adopted edition.

Examine DER and shared services

Review who controls inverter or storage settings, remote management, firmware approval, fleet-level identities, communications, recovery and emergency operating coordination. Determine whether one supplier account can affect multiple sites. Do not issue grid-control commands as a cybersecurity demonstration.

Sources: P06, P07, S08, S42.

Substation and control center examination

Use operating-approved records to follow the path from dispatch and engineering access to a credible grid or plant consequence.

Control centers

Reconcile EMS/DMS services, engineering and operator roles, communications paths, identity dependencies and recovery procedures. Review the approved handling of telemetry failures and inconsistent data. Examine records showing that a critical event reaches the responsible operator.

Protection and substations

Identify gateways, remote access, relay engineering tools, time synchronization and the responsible protection engineer. Review approved settings management and change evidence. A reachable management interface does not prove that a protection setting can be altered or that a grid event will follow.

Plant and station services

Trace DCS, balance-of-plant systems, fuel, cooling, backup power and telecommunications dependencies appropriate to the facility. Identify nuclear, pipeline or other separately regulated boundaries. Record which specialist must review each high-consequence pathway.

Acceptance

The control-center and engineering authorities validate the diagram and consequence assumptions. Preserve discrepancies and access limitations. A laboratory relay or representative controller test must identify firmware, configuration and topology differences from the installed equipment.

Sources: F01, P01, P05, R03.

Power incident and recovery exercise

The following scenario is fictional and does not authorize switching, failover or a live communications interruption.

Scenario

An engineering-support account appears in a remote-access record at an unexpected time. A station reports intermittent visibility. The protection configuration is not yet known to have changed.

Test the operating response

The dispatcher determines the operating response and required communications. The technical lead identifies current evidence, clock differences and the limits of what is known. The protection engineer identifies how to establish configuration integrity through approved evidence.

Test the reporting decision

The compliance owner evaluates applicable NERC incident definitions, DOE-417 categories, state utility reports, nuclear or pipeline obligations and contractual notices. Do not assume that one federal report discharges every other duty or that every event has the same reporting clock.

Test restoration dependencies

Locate the approved recovery sequence, trusted configurations, engineering tools, licenses, spare equipment and vendor support arrangements. Record which steps are only discussed and which have prior test evidence. Assign corrective work for missing dependencies and untested assumptions.

Sources: F04, P01, P04, P05.

Power reporting and recurring calendar

Use the applicable instrument for each event and control population. A calendar copied from another utility can omit different state or registered-function duties.

Calendar item	Record to maintain
NERC requirement schedule	Current standard edition, requirement and part, system population, interval, transition rule, responsible owner and evidence period.
State utility program	Commission rule/order, entity classification, annual filing or exercise requirements, confidentiality procedure and submission receipt.
DOE-417 and other incident reporting	Event category, threshold, clock from current instructions, recipient, authorized reporter, alternate, initial submission and follow-up evidence.
Nuclear or pipeline program	License or current directive, separate system boundary, responsible compliance official and the applicable event criteria.
Engineering change and supplier change	Changed settings, architecture, remote support, equipment family or contract. Review classification, baseline, recovery and requirement mappings before closing the change.

Sources: P01, P03, P04, P05, T03, T05.

Document requests and interviews

Request existing records before proposing a live connection. Ask for enough detail to establish the process and control design, then agree how sensitive records will be exchanged.

Initial evidence request

Request the asset inventory, approved diagrams, process description, current configurations, remote-access arrangements, account owners, maintenance records, backup inventory and restoration evidence. Include EMS and DMS platforms, substation gateways, relays, RTUs, plant DCS, engineering stations, historians, DER controllers and vendor remote access. Ask for the applicable regulatory assessments, prior findings and change history.

Give each request an identifier, purpose, expected owner, time period, format and due date. Allow a supervised review when a copy cannot leave the site. Record evidence not supplied and the effect of that limitation. Never request credentials or live network diagrams through a public inquiry form.

Interviews that test the record

Ask operations what happens if visibility, remote control, communications or a critical vendor service is lost. Ask engineering which installed details differ from the diagram. Ask the identity owner how vendor access is approved and revoked. Ask the recovery owner to identify the evidence of the last restore rather than describe a backup product.

Sampling

Define the control population and sampling rationale. Include material differences in site function, equipment family, criticality, remote access and support arrangements. A sample from one convenient facility does not establish the condition at every remote site. State the sample and the unexamined population in the report.

Readiness evidence

Retain the request register, interview notes with participants and dates, source versions, missing-item log and an agreed set of questions for the field visit. The technical lead checks that an interview statement has not been promoted into a tested fact.

Sources: F01, F03.

Safe work and stop authority

The control center and responsible electrical authority retain switching, dispatch and protection authority. Do not alter relay settings, issue switching commands, trip equipment or test failover in a live grid without an approved operating procedure.

Before connecting anything

Attend the operator safety briefing and follow site access, electrical, hazardous-energy, confined-space and other relevant controls. The operator determines which safety program applies. Cyber credentials do not qualify an assessor to perform electrical switching, enter a confined space or bypass a plant permit.

Verify the asset owner, permitted access point, collection device approval, malware screening, cable path and isolation design. A mirror-port or passive tap design can still change traffic handling, expose sensitive data or affect a network. Obtain approval for its installation and removal.

Define measurable stop conditions

Operations defines the baseline process indicators and limits appropriate to generation, transmission, distribution, protection, dispatch, storage, gas operations and supporting station services. Record the conditions that require stopping: unexpected alarms, impaired communications, controller health changes, operator concern or any departure from the approved method. Do not invent a universal packet rate or tolerance.

Name who can stop work and who can authorize resumption. Any technician may call a safety stop. The operating owner directs the plant response. The assessor must not improvise isolation, reset devices or restart the process to recover the test.

Record the stop and recovery

Log time, activity, observed symptoms, notifications, actions directed by operations and restoration evidence. Preserve available records without delaying safety response. Quarantine the activity permit until operations and the technical lead review the cause. Reauthorize only the changed method and remaining targets.

Sources: F01, F03, F06.

Inventory and process dependencies

Build an inventory that explains how assets support generation, transmission, distribution, protection, dispatch, storage, gas operations and supporting station services. A list of IP addresses alone is insufficient.

Use existing evidence first

Reconcile engineering inventories, configuration exports, approved drawings, maintenance records and supervised physical observations. Record asset identifier, function, location, owner, manufacturer, model, firmware/software, support status, protocol, zone and recovery dependency. Distinguish observed values from information supplied by a vendor or operator.

Trace the consequence

For each critical process, trace the route from operator interface and control logic to communications, field equipment and supporting services. Identify how an asset failure could contribute to loss of situational awareness, incorrect switching, impaired protective operation, generation interruption or a wider supply disturbance. Ask engineering to validate the consequence and available protection or manual alternatives.

Record protective functions separately from normal process control. Document dependencies on identity, time sources, licensing, cloud support, third-party communications and engineering tools. Do not assume a safety function remains independent because it appears in a different diagram layer.

Resolve discrepancies

Mark unknown devices, duplicated identifiers, obsolete drawings and unverified vendor assets. Ask the owner to resolve the discrepancy. An unsupported system needs a control and recovery decision; it is not automatically safe to patch, scan or replace during the assessment.

Acceptance

The asset owner signs the scoped inventory and dependency map. The report states the sources, collection date, completeness limits and unresolved high-consequence dependencies. Sensitive addressing and configuration details belong in the controlled technical appendix.

Sources: F01, R01, R02.

Network paths and remote access

Review the paths by which a person, service or external system can reach the scoped process. A firewall diagram is a hypothesis until its relevant controls and limitations are examined.

Examine the intended boundary

Use dated configurations, rules, diagrams and approved architecture records to identify zones, conduits, remote entry points, jump services and management interfaces. Record source, destination, permitted service, business purpose, approver and review date for each material path.

Separate corporate identity, vendor support, telemetry, cloud management and emergency access. Check whether access can be limited to named users and required assets, reviewed, recorded and revoked. Examine an actual approval and revocation sample rather than relying only on a written policy.

Examine the actual access process

Observe a supervised approved support workflow or review retained session records. Record authentication, authorization, account ownership, session visibility, shared-account constraints and timeout or revocation behavior. Where an old controller cannot support the desired mechanism, evaluate controls at an approved access gateway.

Prove only what the method establishes

Configuration review can identify an allowed policy path but may not prove live reachability or exploitation. A controlled connectivity check is a separate authorized activity. A proposed segmentation improvement remains a recommendation until implemented and verified.

Required records

Retain the approved path register, source versions, access samples, exceptions and the method used. If ISA/IEC 62443 is contractual, obtain the licensed edition and agreed assessment criteria before claiming conformity. The publicly described zone/conduit approach is not a certification.

Sources: F01, F08.

Accounts legacy systems and suppliers

Start with the access needed to operate and recover the process. Identify the controls that the installed system can support and the protections applied around it.

Accounts and authorization

Review named users, service accounts, vendor accounts and emergency credentials through approved records. Verify owners, privileges, approval, periodic review and revocation evidence. Review how privileged access is separated from normal user activity. Do not collect secrets in the evidence register.

For shared or embedded accounts, document the technical limitation and compensating controls. Record who knows the credential, how access is supervised and logged, how access is removed when people leave, and what change process is needed to reduce reliance on the account.

Support and vulnerability decisions

Match versions and support status to vendor advisories and approved evidence. Separate a version match, a suspected vulnerability, and a validated condition. A scanner finding against a similar product does not establish the condition of the installed controller.

For a legacy device, compare patch availability, vendor support, maintenance dependencies, network exposure, replacement lead time and restoration options. The assessment recommends a decision. Operations and engineering approve changes under their change process.

Supplier obligations

Review contracts for remote access, notification, vulnerability handling, evidence availability, subcontracting, licensing and exit support. Identify unsupported promises and dependencies that have no named owner. Include a supplier contact and escalation alternate in the operating handover.

Sources: F01, F08.

Monitoring time and evidence handling

Establish whether the available records can answer who accessed what, when, through which path and with what effect. Preserve time uncertainty rather than changing production clocks.

Collect a usable record

Identify event sources, collection routes, retention settings, access restrictions and review responsibility. Include jump-host, authentication, firewall, engineering and system records relevant to the scoped process. Verify a small authorized event sample appears at the intended collection point.

Record timezone, clock source, observed offset and known gaps. If clocks disagree, preserve the original timestamps and the translation used in analysis. A missing event may be a collection limitation rather than proof that an action did not happen.

Evidence integrity

Assign a stable evidence ID. Record origin, custodian, collection date and method, source period, filename or record reference, integrity value where appropriate, storage location and access history. Keep originals protected and conduct analysis on controlled working copies. Log transformations and redactions.

Sensitive information

Have the compliance owner classify customer information, engineering records and any SSI, CEII, CUI or protected public records. Use the handling rules that actually apply. A confidentiality label alone does not establish legal privilege or a statutory disclosure exemption.

Acceptance

The custodian verifies access, recoverability and retention against the applicable instrument or agreed contract. Do not use one generic retention period for every regulator. Preserve incident records and any legal hold independently of the normal assessment deletion date.

Sources: F01, F03, F04.

Recovery and continuity evidence

Check whether the operator can restore the process after loss of EMS and DMS platforms, substation gateways, relays, RTUs, plant DCS, engineering stations, historians, DER controllers and vendor remote access. Backup-job success alone does not establish recovery capability.

Define the restoration objective

Ask operations to identify the minimum service, safe process condition, restoration sequence and maximum tolerable interruption. Record the chosen recovery objectives, their owner and the evidence supporting feasibility. Do not substitute a generic IT recovery target for an operating requirement.

Examine recovery dependencies

Identify controller and server configurations, engineering projects, firmware, software, licenses, keys held in controlled storage, approved hardware, spare components and vendor support. Determine whether a clean engineering station and trusted installation material will be available during an incident.

Review backup isolation, access, integrity checks and the evidence of a representative restore. A production controller upload, download or failover requires a separately approved activity. Prefer an appropriate isolated or representative system when production work is unsuitable.

Exercise and validate

Use a scenario with loss of a material dependency. Record which recovery steps were discussed, demonstrated in a representative environment or performed in production under approval. Document differences between the test environment and the installed system. A tabletop exercise does not prove a successful technical restore.

Closure evidence

Retain the recovery procedure version, scenario, approvals, result, elapsed time if actually measured, unresolved dependencies and corrective owner. Operations accepts the restored state. Untested assumptions remain explicit in the report and recurring program.

Sources: F01, F04, R03.

Authorization for active validation

Active validation is optional until a controlling requirement or agreed scope requires it and an acceptable method is authorized. A contractual requirement does not remove the need for a safe operating method.

Write an activity permit

Identify exact targets, system owner, purpose, tool and version, commands or test functions, allowed traffic behavior, exclusions, operating window and collection location. Include vendor restrictions, communications, recovery support and evidence to retain. Approve the method for the installed version rather than a similar laboratory device.

Choose the least disruptive evidence

Consider configuration examination, supervised control demonstration, existing logs and representative-environment validation before a production probe. Record which requirement each method addresses and what it cannot establish. Peer reviewed testbed research helps explain test design but does not prove production safety.

Confirm readiness at the point of work

Operations confirms the process condition and baseline indicators. The technical lead confirms approved tool settings and targets. The evidence custodian confirms recording. The project manager verifies that the authorization is current and that the named stop authority is reachable.

Do not perform denial-of-service, fuzzing, credential guessing, exploit execution, firmware change, controller write or failover merely because it is a standard scanner option. A necessary activity needs an explicit method, suitable environment and separate approval.

Close the permit

Record start and end times, targets actually reached, deviations, stops, observations and operating-owner acceptance. Revoke temporary access and remove approved collection equipment using the agreed procedure. Keep the original permit and test record linked to the finding.

Sources: F01, F03, R03.

Writing findings that can be audited

A finding must show the condition, its evidence, the applicable criterion and the significance for the process. Keep observed facts separate from possible operating consequences.

Minimum finding record

Record the finding ID, asset or control boundary, evidence IDs and dates, requirement or agreed criterion, observed condition, method and limitation. Explain the credible operating consequence and assumptions. Record existing safeguards, recommended action, responsible owner and proposed verification method.

Use precise status

Use Observed when the available evidence establishes a condition. Use Suspected or Unresolved when it does not. Record a recommendation, implementation and verification as separate states. A screenshot of a configuration change may support implementation without proving that the intended boundary works.

Prioritize consequence and uncertainty

Evaluate potential effects on generation, transmission, distribution, protection, dispatch, storage, gas operations and supporting station services, exposure paths, existing safeguards, recovery limits and confidence in the evidence. Include loss of situational awareness, incorrect switching, impaired protective operation, generation interruption or a wider supply disturbance where the process supports that consequence. Have engineering review the pathway before presenting it as a fact.

A CVSS score can help describe a software vulnerability, but it does not replace process consequence analysis. Record the organization's risk method and acceptance authority. Avoid multiplying arbitrary numbers into an apparently precise plant-risk score.

Resolve challenge

Give the operating owner a chance to identify incorrect asset facts, missing safeguards and unsafe remediation proposals. Retain the challenge, additional evidence, reviewer decision and revised wording. A disagreement is not closed merely because the report was delivered.

Sources: F01, R01, R02.

Corrective work and management reporting

The assessment ends with decisions that an owner can implement and a reviewer can verify. A long list of vulnerabilities without an operating sequence is not a corrective plan.

Plan the work

For each accepted finding, identify the owner, dependency, required design or procurement, change approval, maintenance window, recovery support, target date and verification evidence. Identify an interim control if the final fix cannot be completed promptly. Do not label a deferred action Implemented.

Sequence actions by operating consequence and dependency. An access boundary may need a maintained jump host, named accounts and supplier support before a legacy controller can be isolated. Verify that the proposed change does not prevent emergency operation or recovery.

Report to leadership

Provide a concise operating-risk summary, the most consequential unresolved issues, funding or outage decisions, affected services and the limits of the assessment. Show the remaining work and who may accept the residual risk. Keep confidential addressing and detailed weaknesses in a restricted appendix.

Report to technical owners

Provide enough evidence and context to reproduce the observation using the approved method. Identify configuration versions, affected boundary, exceptions and exact acceptance criteria. Do not include reusable credentials or unnecessary customer information.

Regulatory conclusion

State only the obligations actually assessed, versions, facility scope, sample and dates. List requirements not assessed or not demonstrated. An engineering assessment does not certify overall organizational compliance or replace a regulator's decision.

Sources: F01, F03.

Verification closure and recurring work

Close an action against predefined evidence. A management assertion, purchase order or completed ticket is not automatically a verified control result.

Verification procedure

The reviewer checks that implementation evidence matches the approved change. Agree a safe validation method, compare the result with the acceptance criterion, and retain the evidence. Record exceptions and whether the result establishes design, implementation or operating effectiveness.

If production validation remains unsuitable, state what the alternative evidence supports and what remains uncertain. The risk owner may accept that limit within delegated authority; the report must not silently convert it into a tested result.

Handover

Return the current inventory, dependency map, control and finding register, activity permits, relevant evidence index, operating procedures, supplier contacts and training record to the designated owners. Check that records can be retrieved by authorized staff during an outage. Remove temporary access under the agreed change record.

Recurring triggers

Schedule reviews from the actual instruments and operational change cycle. Trigger a new applicability review after ownership or service changes, a new state footprint, contract changes, a revised standard, significant architecture change or a material incident. Confirm whether a statutory update or certification is required before setting the due date.

Final acceptance

The operating owner accepts the process condition and handover. The technical reviewer signs the evidence-based conclusions. The compliance owner approves the requirement mapping and remaining legal questions. The sponsor records funding and residual-risk decisions. The project manager closes only the deliverables that meet those acceptance criteria.

Sources: F01, F03, F04.

Facility and applicability worksheet

Complete one worksheet for each legal entity, facility and distinct regulatory boundary. Keep source records in controlled storage.

Facility legal entity address and operating function

Ownership operator classification permits registration and contracts

Applicable instruments exact versions and source record IDs

Applicability decisions exceptions and unresolved questions

Operating technical compliance and project owners with alternates

Decision approvers dates next review and authority record

Field activity authorization worksheet

The operating owner approves the activity before work. This worksheet records permission; completing it does not itself grant authority.

Activity purpose exact targets and asset owners

Method tool version permitted functions and excluded actions

Vendor constraints approved traffic behavior and operating baseline

Operating window communications and named stop authority

Recovery support safe response and resumption authority

Operating approval technical approval date and change record

Evidence and finding worksheet

Record facts separately from possible consequences. Link the original evidence and preserve source times and limitations.

Evidence ID source custodian period collection method and integrity

Observed condition and method used to establish it

Applicable requirement exact version and agreed assessment criterion

Operating consequence safeguards assumptions and evidence limits

Finding ID responsible owner priority rationale and challenge

Reviewer disposition date and linked technical record

Corrective action and acceptance worksheet

Keep recommended, implemented and verified states separate. Record remaining risk and the person authorized to accept it.

Finding ID action owner dependencies and target date

Approved implementation change record and operating window

Verification criterion authorized method result and evidence IDs

Remaining limitations interim controls and residual risk decision

Operating acceptance compliance disposition and recurring review

Technical reviewer sponsor decision date and closure record

Terms used in the planning records

Term	Meaning in this pack
OT ICS and SCADA	Operational technology; industrial control systems; supervisory control and data acquisition.
PLC RTU HMI DCS SIS	Programmable logic controller; remote terminal unit; human-machine interface; distributed control system; safety instrumented system.
RRA ERP and PWSID	Risk and resilience assessment; emergency response plan; public water system identifier.
BES CIP DER and EMS DMS	Bulk Electric System; Critical Infrastructure Protection; distributed energy resources; energy/distribution management system.
SSI CEII and CUI	Sensitive Security Information; Critical Energy/Electric Infrastructure Information under the applicable authority; Controlled Unclassified Information. Determine the actual handling regime.
CySO CISO and EHS	Cybersecurity Officer; Chief Information Security Officer; environment health and safety.
PHA MOC and CMMC	Process hazard analysis; management of change; Cybersecurity Maturity Model Certification.
Applicable and Unresolved	Applicable requires facility facts and a controlling instrument. Unresolved identifies a missing fact or authority; it is not equivalent to Not applicable.

Sources and instrument status

F01 Guide to Operational Technology Security Revision 3

NIST. Final guidance. September 2023 final publication; chapters 4 through 6 and OT control tailoring.

F02 Guide to Operational Technology Security Revision 4

NIST. Draft guidance. September 21 2026 initial public draft. Revision 4 is not the final baseline in this edition.

R01 A survey of cyber security management in industrial control systems

Knowles and colleagues in International Journal of Critical Infrastructure Protection. Peer reviewed research. Volume 9 June 2015 pages 52 to 80. Used for qualitative management context, not contemporary law or numeric effectiveness claims.

R02 Threat modeling of industrial control systems A systematic literature review

Computers and Security. Peer reviewed research. Volume 136 January 2024 article 103543. Supports structured threat modeling; it does not validate a specific plant assessment.

R03 ICSSIM A framework for building industrial control systems security testbeds

Computers in Industry. Peer reviewed research. Volume 148 June 2023 article 103906. Laboratory results do not establish safety or coverage on installed production equipment.

Sources: F01, F02, R01, R02, R03.

Sources and instrument status

F03 Technical Guide to Information Security Testing and Assessment

NIST. Final guidance. Assessment planning and rules of engagement. Apply OT operating constraints; this IT testing guide does not authorize production testing.

F05 CIRCIA public rulemaking notice

CISA and Federal Register. Rulemaking record. 2026 notice referring to the proposed rule and further town halls. This notice does not establish an effective final reporting rule. A current final rule was not established in this research.

F09 Cybersecurity Resource Center

New York DFS. Agency implementation source. 23 NYCRR Part 500 covered entity scope. New York location alone does not make an industrial operator a DFS covered entity.

P01 Critical Infrastructure Protection reliability standards register

NERC. Standards register. Family status and mandatory versus future enforcement. Freeze the exact applicable standard, requirement and US implementation plan for the engagement. Approval and enforcement dates differ.

P02 New bulk power reliability safeguards

FERC. Agency order announcement. March 19 2026 approvals including virtualization and low impact controls. Use the underlying orders and implementation plans; the announcement is not a universal immediate enforcement date.

Sources: F03, F05, F09, P01, P02.

Sources and instrument status

P03 Reliability standards and US effective date resources

NERC. Standards register. US effective date status and functional applicability.

P05 Nuclear cybersecurity

NRC. Agency implementation source. 10 CFR 73.54 and approved licensee cybersecurity plans. Nuclear licensing scope is separate from NERC CIP scope.

P06 Electric distribution cybersecurity baselines

NARUC and DOE. Government supported guidance. Distribution and distributed energy resource baselines. Not a nationwide binding rule; identify state adoption or contract incorporation.

P07 Utility IT cybersecurity regulations announcement

New York DPS. Agency announcement. April 16 2026 announcement; June 1 2026 effectiveness. The announcement explicitly distinguishes IT regulations from prospective industry OT rulemaking.

S08 Delaware selected authority

Delaware PSC. Regulator program. Selected state authority and applicability research as of October 16 2026.

Sources: P03, P05, P06, P07, S08.

Sources and instrument status

S42 Tennessee selected authority

Tennessee Secretary of State. Filed utility rule. Selected state authority and applicability research as of October 16 2026.

F04 Incident Response Recommendations and Considerations Revision 3

NIST. Final guidance. April 2025 final publication.

P04 Electric Emergency Incident and Disturbance Report

DOE. Agency reporting source. Current DOE-417 form and event instructions. Determine the applicable incident category and clock from current instructions; no single clock covers all events.

T03 Pipeline Cybersecurity Mitigation Actions Contingency Planning and Testing

TSA. Expired directive copy. Security Directive Pipeline-2021-02F; effective May 3 2025; expires May 2 2026. Historical public reference only. Obtain the currently issued instrument and applicability notice from the operator.

T05 Pipeline control room management

PHMSA. Agency implementation guidance. 49 CFR 192.631 and 195.446; controller and SCADA scope. These are safety requirements alongside any applicable TSA cybersecurity instrument.

Sources: S42, F04, P04, T03, T05.

Sources and instrument status

F06 State Plans

OSHA. Jurisdiction directory. State and federal occupational safety jurisdiction. Check public employee coverage and industry exceptions for the actual workplace.

F08 ISA IEC 62443 Series of Standards

ISA. Standards publisher overview. Published series and applicable parts. Full normative texts were not obtained. No clause-level conformity or security level is certified here.

Sources: F06, F08.