GLOBAL DIGITAL FORENSICS

OT ASSESSMENT PLANNING PACK

Power and Energy OT Assessment Planning Pack

Power and energy operational technology, industrial control systems and SCADA

Edition 2026-11-03 | November 3, 2026

Plan the assessment, settle which obligations apply, collect traceable evidence, protect operating authority and carry corrective work through verification and handover.

Use the project workbook for applicability, work planning, evidence, findings, local duties and notifications. The worksheets in this pack print for field use.

Questions about this document: call (800) 868-8189 or write to info@evestigate.com.

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

Contents

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

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

What this pack covers

This pack plans an OT security assessment of generation, transmission, distribution, protection, dispatch, storage, gas operations and station services across the United States. Use it with the project workbook and the state and local research companion.

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 printable worksheets carry the work from planning through handover.

How current the guidance is

Regulatory statements are current to November 3, 2026. Each names its source in the register at the end of the pack, linked to the issuing authority. Permits, operator directives and contracts add duties that only your own records show, so the workbook asks for them by name.

Standards behind the method

The method follows NIST SP 800-82 Revision 3 for OT security and NIST SP 800-115 for test planning. Where a contract or regulator calls for ISA/IEC 62443, the work maps to 62443-2-1 for the asset owner security program, 62443-3-2 for risk assessment with zones and conduits, and 62443-3-3 for system security requirements and security levels.

Sign off

Your operating, technical and compliance owners sign the facility records before the organization adopts the conclusions. GDF examiners can run the assessment, review your records or support your own team.

Sources: F01, F03, F08

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 starting 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.

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

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 collects evidence; obligations come from the governing instruments.

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. Take deadlines from effective and compliance dates.

Signing an assessment conclusion

The reviewer needs the actual facility facts, current instruments, examined evidence, test permissions and unresolved limitations. A designated technical reviewer reviews the completed work, and the organization then 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. Each system carries its own 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 outstanding 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. Approval is express.

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

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. Alter relay settings, issue switching commands, trip equipment or test failover in a live grid only with 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. The operating owner sets the target list and authorizes active tests.
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 postwork operating acceptance. Record the validation scope that was authorized.
5 Reporting and decisions	Reviewed findings, requirement mappings, limitations, corrective owners, funding decisions and a residual risk record.

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

Stage	Required exit evidence
6 Verification and handover	Retest evidence, recurring review schedule, retained records, lessons and signed handover. Recommendations close when 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.

Mark an item Not applicable on a documented basis. 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. Independently applicable federal obligations continue.

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 follows from the entity's actual operations.

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

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. Take enforceability from the implementation plan's effective date.

Other energy boundaries

Review distribution only systems, DER, gas operations and pipelines on their own rules. 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. A complete CIP compliance conclusion for an item rests on its current standard and a settled boundary.

Sources: P01, P02, P03, P05

NERC CIP versions in force

Record the enforceable version of each CIP standard on the audit date. Two recent orders change the set.

Order No. 919 (virtualization)

FERC Order No. 919 approved CIP-002-7, CIP-003-10, CIP-004-8, CIP-005-8, CIP-006-7.1, CIP-007-7.1, CIP-008-7.1, CIP-009-7.1, CIP-010-5, CIP-011-4.1 and CIP-013-3; CIP-002-8 and CIP-003-11 were approved in separate concurrent orders. The rule took effect May 26, 2026. The standards take effect on the later of April 1, 2026 or the first day of the first calendar quarter 24 months after the order took effect, and entities may adopt them early. Until then, audit against the versions currently enforceable and note which controls change with virtualization.

CIP-015-1 internal network security monitoring

CIP-015-1 internal network security monitoring (Order No. 907) takes effect October 1, 2028 for Control Centers and backup Control Centers with high or medium impact BES Cyber Systems, and 24 months later for other medium impact BES Cyber Systems with external routable connectivity. Plan the monitoring data feeds and baselines now. Order No. 907 approved the standard effective September 2, 2025, and directed NERC to extend monitoring to EACMS and PACS outside the electronic security perimeter.

Sources: P01, P02, P09, P10

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

CIP evidence workstreams

Use these as candidate evidence workstreams. Each row starts with the applicable requirement, version, system and population.

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. Apply low impact requirements 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. A completed test record is where we look for evidence of technical recovery.
Configuration and vulnerability work	CIP-010 where applicable. Link baseline, change and assessment evidence to the named system and requirement. Map each required method to its own evidence.
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 govern a scoped system outside NERC CIP.

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. Scope OT assessment duties from OT instruments. Delaware describes annual Class A utility cyber filings. Tennessee and other states have separate utility programs that need current scope and filing checks.

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

Use guidance appropriately

The NARUC and DOE distribution baselines can support a gap assessment when agreed by the owner. They serve as guidance for distribution systems. 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. Grid control commands stay with system operators.

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 marks a path to examine further.

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 runs as a discussion with systems in normal operation.

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

Scenario

An engineering support account appears in a remote access record at an unexpected time. A station reports intermittent visibility. Confirm the protection configuration against baseline.

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. Track each reporting duty and clock on its own, alongside any federal report.

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

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

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. Offer supervised onsite review when copies stay onsite. Record outstanding evidence and its effect on the conclusion. Exchange credentials and live diagrams through secure channels.

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. Draw samples across remote sites so the result describes the whole population. 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. Alter relay settings, issue switching commands, trip equipment or test failover in a live grid only with an approved operating procedure.

Connecting equipment safely

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. Electrical switching, confined space entry and plant permits stay with personnel qualified and authorized for them.

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

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. Set packet rates and tolerances from device specifications.

Name who can stop work and who can authorize resumption. Any technician may call a safety stop. The operating owner directs the plant response. Plant operators handle isolation, device resets and process restart under their recovery procedure.

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. Confirm safety function independence from actual connections.

Resolve discrepancies

Mark unknown devices, duplicated identifiers, obsolete drawings and unverified vendor assets. Ask the owner to resolve the discrepancy. An unsupported system gets a control and recovery decision; patching, scanning or replacing it follows an approved operating method.

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

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 lacks the desired mechanism, evaluate controls at an approved access gateway.

Report what the method tested

Configuration review identifies allowed policy paths; approved validation tests 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 and conduit approach is a design method.

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.

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

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. Store secrets by reference 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. Confirm a scanner finding against 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 reflect a collection gap; check logging coverage.

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.

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

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. Privilege and disclosure exemptions rest on their legal tests.

Acceptance

The custodian verifies access, recoverability and retention against the applicable instrument or agreed contract. Set retention periods regulator by 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. Restore tests are where we look for evidence of 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. Set recovery targets from the 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 tests decisions; restore tests are where we look for evidence of recovery.

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

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

Authorization for active validation

Active validation is optional until a controlling requirement or agreed scope requires it and an acceptable method is authorized. Meet every contractual requirement with 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 the scope of what it shows. Peer reviewed testbed research informs test design.

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.

Run denial of service, fuzzing, credential guessing, exploit execution, firmware change, controller write or failover only under explicit approval for that method. 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.

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

Use precise status

Use Observed when the available evidence establishes a condition. Use Suspected or Unresolved otherwise. 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 describes a software vulnerability; consequence analysis is where we assess the plant impact. Record the organization's risk method and acceptance authority. Keep plant risk ratings as precise as the evidence behind them.

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 closes with a recorded resolution.

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 corrective plan sequences vulnerabilities into operating steps.

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 while the final fix is scheduled. Mark an action Implemented once the work is done.

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 preserves emergency operation and 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. Include only data the task requires, through approved channels.

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

Regulatory conclusion

State only the obligations actually assessed, versions, facility scope, sample and dates. List requirements not assessed or not demonstrated. An engineering assessment informs organizational compliance decisions and the regulator's own decision.

Sources: F01, F03

Verification closure and recurring work

Close an action against predefined evidence. Verify the control directly; tickets and assertions point to where to look.

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.

Where production validation is unsuitable, state what the alternative evidence supports and the confidence it carries. The risk owner may accept that limit within delegated authority, and the report states it as accepted rather than tested.

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 any statutory update or certification duty, then set 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.

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

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 that the authorizing official grants.

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

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

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

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

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; Not applicable records a supported basis.

Sources

Each source is linked to the issuing authority or publisher. The date shows when the entry was last checked.

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

F01 Guide to Operational Technology Security Revision 3. NIST. Final guidance. September 2023 final publication; chapters 4 through 6 and OT control tailoring. https://csrc.nist.gov/pubs/sp/800/82/r3/final (checked October 15, 2026)

F02 Guide to Operational Technology Security Revision 4. NIST. Draft guidance. September 21 2026 initial public draft. Initial public draft dated September 21, 2026; comments are due November 30, 2026. Revision 3 is the final guidance. https://csrc.nist.gov/pubs/sp/800/82/r4/ipd (checked October 15, 2026)

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. https://doi.org/10.1016/j.ijcip.2015.02.002 (checked October 15, 2026)

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 for use in a specific plant assessment. https://doi.org/10.1016/j.cose.2023.103543 (checked October 15, 2026)

R03 ICSSIM A framework for building industrial control systems security testbeds. Computers in Industry. Peer reviewed research. Volume 148 June 2023 article 103906. Confirm safety and coverage on installed production equipment. https://doi.org/10.1016/j.compind.2023.103906 (checked October 15, 2026)

F03 Technical Guide to Information Security Testing and Assessment. NIST. Final guidance. Assessment planning and rules of engagement. Apply OT operating constraints; the operating owner authorizes production testing. https://csrc.nist.gov/pubs/sp/800/115/final (checked October 15, 2026)

F05 CIRCIA public rulemaking notice. CISA and Federal Register. Proposed rule; final rule under White House review since October 1, 2026. 2026 notice referring to the proposed rule and further town halls. Reporting clocks start when the final rule takes effect. https://public-inspection.federalregister.gov/2026-10417.pdf (checked November 3, 2026)

F09 Cybersecurity Resource Center. New York DFS. Agency implementation source. 23 NYCRR Part 500 covered entity scope. DFS coverage rests on a Banking, Insurance or Financial Services Law authorization. https://www.dfs.ny.gov/industry_guidance/cybersecurity (checked October 15, 2026)

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. https://www.nerc.com/standards/reliability-standards/cip (checked October 15, 2026)

P02 Order No. 919, Critical Infrastructure Protection Reliability Standards. FERC, Federal Register. Final rule. Approves CIP-002-7, CIP-003-10, CIP-004-8, CIP-005-8, CIP-006-7.1, CIP-007-7.1, CIP-008-7.1, CIP-009-7.1, CIP-010-5, CIP-011-4.1 and CIP-013-3; rule effective May 26, 2026; standards effective on the later of April 1, 2026 or the first day of the first calendar quarter 24 months after the order takes effect. https://www.govinfo.gov/content/pkg/FR-2026-03-24/html/2026-05716.htm (checked November 3, 2026)

P03 Reliability standards and US effective date resources. NERC. Standards register. US effective date status and functional applicability. https://www.nerc.com/standards/reliability-standards (checked October 15, 2026)

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. https://www.nrc.gov/facilities-safety/cybersecurity (checked October 15, 2026)

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

P09 Order No. 907, CIP-015-1 Internal Network Security Monitoring. FERC, Federal Register. Final rule. Approves CIP-015-1; rule effective September 2, 2025. https://www.govinfo.gov/content/pkg/FR-2025-07-02/html/2025-12309.htm (checked November 3, 2026)

P10 CIP-015-1 implementation plan, Project 2023-03. NERC. Approved implementation plan. Effective the first day of the first calendar quarter 36 months after the approving order takes effect (October 1, 2028) for Control Centers and backup Control Centers identified under CIP-002 R1.1 and R1.2; other medium impact BES Cyber Systems with external routable connectivity 24 months later. https://www.nerc.com/pa/Stand/Project_202303_INSM_DL/2023%2003%20Implementation%20Plan%20clean_Feb2024.pdf (checked November 3, 2026)

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. https://pubs.naruc.org/pub/364B7A14-D21C-D2DF-BB6B-FFF3F93E1D51 (checked October 15, 2026)

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. https://dps.ny.gov/node/29056 (checked October 15, 2026)

S08 Delaware starting source. Delaware PSC. Regulator program. State authority and applicability sources current to October 15, 2026. https://depsc.delaware.gov/cybersecurity/ (checked October 15, 2026)

S42 Tennessee starting source. Tennessee Secretary of State. Annual utility cybersecurity filing docket. TPUC Docket 26-00047 documents 2026 annual confidential utility cybersecurity filings, including water, wastewater and gas providers. This records current implementation; scope exceptions, the July 1 deadline and incident clocks come from the rule text. Authenticate the current codified chapter 1220-04-15 from the official code. Use the adopted rule and this utility's own filing. https://publications.tnsosfiles.com/rules_filings/06-31-23.pdf (checked October 17, 2026)

F04 Incident Response Recommendations and Considerations Revision 3. NIST. Final guidance. April 2025 final publication. https://csrc.nist.gov/pubs/sp/800/61/r3/final (checked October 15, 2026)

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. https://doe417.energy.gov/ (checked October 15, 2026)

T03 Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing. TSA. Current security directive. Security Directive Pipeline-2021-02G, effective May 3, 2026 through May 2, 2027; cancels and supersedes Pipeline-2021-02F; owners and operators of hazardous liquid and natural gas pipelines and LNG facilities notified by TSA. https://www.tsa.gov/sites/default/files/signed_security_directive_pipeline-2021-02g_and_transmittal_memo_508c.pdf (checked November 3, 2026)

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. https://www.phmsa.dot.gov/pipeline/control-room-management/control-room-management (checked October 15, 2026)

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

F06 State Plans. OSHA. Jurisdiction directory. State and federal occupational safety jurisdiction. Check public employee coverage and industry exceptions for the actual workplace. https://www.osha.gov/stateplans/ (checked October 15, 2026)

F08 ISA IEC 62443 Series of Standards. ISA. Licensed standards series. 62443-2-1 security program for asset owners; 62443-3-2 security risk assessment, zones and conduits; 62443-3-3 system security requirements and security levels; 62443-4-2 component requirements. Use the licensed edition named in the contract when conformity to a part is required. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (checked October 15, 2026)

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

Plan the assessment with a senior examiner

GDF plans and runs OT and SCADA security assessments for operators of critical infrastructure. On the first call a senior examiner reviews your facilities, the obligations that apply, operating windows and what the assessment must prove, then recommends the scope and testing depth.

Get a free consultation. The initial consultation is free, and requests are handled in confidence.

Call (800) 868-8189 at any hour, or write to info@evestigate.com.

Request a consultation online at evestigate.com/contact.

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