Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/power-energy-assessment-manual/

POWER AND ENERGY OT ASSESSMENT PLANNING MANUAL

Power and Energy OT Manual, NERC CIP Scope First

BES Cyber System status comes from registration and categorization, and switching commands stay with the control center whatever an assessment finds. This manual from Global Digital Forensics helps registered entities, distribution utilities, generators and their advisers settle scope on those terms before anyone touches a relay.

Planning scope and research basis

This manual is built for a controlled assessment of generation, transmission, distribution, protection, dispatch, storage, gas operations and supporting station services at facilities in the United States. It carries the federal, bulk power and sector research; the companion volume screens all fifty states so you can resolve the commission orders, public power rules and contract terms that set the duties for systems outside NERC CIP applicability.

What the assessment produces

An approved scope, an applicability register, a process dependency map, examined evidence, safe activity records, consequence based findings, a corrective plan and a verification record. The workbook and the fillable worksheets carry the work from planning through handover, and every output has a named owner before the first substation visit is scheduled.

Sources current to November 3, 2026

Current public primary sources, official program material and selected peer reviewed research support the text. Effective instruments take precedence over guidance and over this manual. The licensed ISA/IEC 62443 parts, operator security directives, facility permits and private contracts are held by the organization itself, so the utility's own registration, categorization and commission filings are the first records the assessment requests.

Open applicability

The source register gives binding instruments, guidance, drafts, superseded versions and open questions their own entries. Each open entry points to the controlling text and the facility facts to gather, and gathering them prepares the site specific conclusion for signature.

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

Adoption and review

Complete the facility specific records and obtain the named operating, technical and compliance approvals. The questions that settle each date, threshold and clause are summarized in OT questions to settle before field work.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-82 Rev. 4 initial public draft, Guide to Operational Technology (OT) Security (F02), A survey of cyber security management in industrial control systems (R01), Threat modeling of industrial control systems: A systematic literature review (R02), ICSSIM: A framework for building industrial control systems security testbeds (R03)

To settle whether a registered function or a commission order governs the system in front of you, describe the entity and the facilities to a senior examiner before the applicability register is drafted.

Applying the Updated Audit Workbook

The workbook works as an execution record rather than a checklist. Every procedure row now carries the fields an auditor will read first: the exact criterion tested, the population it was tested against, the period, the sampling rationale, the permitted method, the execution date, the actual observation, the evidence identifiers and the reviewer. A row with those fields completed is a result, a row in progress is a plan, and the workbook keeps the two visibly apart.

Pre Execution Readiness Checklist

Fill the criterion, population, period and sampling rationale before anyone touches a system, because those four fields give the eventual observation its meaning. Record the permitted method exactly as the activity permit states it. When the work is done, enter the execution date, what was actually observed and the evidence identifiers that support it, then hand the row to the named reviewer. Keep the source register and the operating authority record apart from the procedure rows, so the auditor reads the legal citations and the operating approvals as separate records.

Pending Scope and Governance Decisions

The open count on the Start sheet tracks blank decisions, decision text that needs correcting and resolved selections awaiting a required record field. Treat Fields present as the prompt for qualified review, and treat completion as the point when that review is signed. The responsible operating, technical and compliance people fill the approval fields once they have reviewed the work, and those signatures are what mark a workbook as reviewed rather than simply filled.

Engagement Scope and Authorization

Record every proposed exclusion, its reason and the responsible reviewer in Scope decisions so deferred work stays visible to the sponsor. The State research sheet is a separately labelled routing register: its state and sector rows are a client research checklist, and a row becomes part of a facility conclusion once the

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

controlling instrument is retrieved and recorded beside it. For New York work use the Clause matrix and questions Q01 to Q10 in the New York set. A current instrument or local fact that is being gathered stays marked Unresolved, and the mark changes when someone retrieves the text or establishes the fact.

Source Access and Revision History

The Sources sheet lists each source with the date it was reviewed. Request the current text of each source as you reach it, and keep the duty on the register while the text is on its way. Use the Edition record to track your own revisions and reviews, and keep the previous version when you adopt a new one.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

Using this planning pack

Use this pack in the order a utility makes decisions. Fix the legal and operating boundary first, because the registered function, the BES Cyber System categorization and the commission jurisdiction decide which duties attach to generation, transmission, distribution, protection, dispatch, storage, gas operations and station services. Choose evidence and methods once the control center and the responsible electrical authority have agreed what may be examined, so the assessment informs the grid while operators keep full control of it.

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's state and sector rows form a client research checklist, with a separate register of fifty state starting sources; a row becomes a facility determination when the operator records the instrument and the decision beside it. Appoint a sponsor, an operating owner, a technical lead, a compliance owner and a project manager. Complete the site worksheet. Resolve the mandatory instruments and the operating permissions before scheduling any intrusive work, and 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. A procedure description explains how the assessment team can collect evidence, and the legal obligations themselves come from the cited instruments. A rule can be effective while a particular requirement carries a later compliance date, and an approved standard can be subject to future enforcement. Record both dates and the applicable version, and take each deadline from the instrument's effective date.

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

Before signing an assessment conclusion

The reviewer works from the actual facility facts, the current instruments, the examined evidence, the test permissions and the recorded open items. Preparing this pack readies the record, and the assessment itself is what examines the facility. A named technical reviewer reviews the completed work before the organization adopts or publishes its conclusions.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

Keep the workbook field guide beside the pack while the first facility record is created, and let the open rows set the agenda for the first planning call.

Decisions before mobilization

Separate the registered bulk power functions and BES Cyber Systems from distribution only systems, DER, gas facilities, pipelines and nuclear licensed systems before any checklist is opened. Each of these systems carries its own obligations under a common corporate owner, and a register that keeps them apart is the register an auditor can follow.

Define the work product

Decide in writing whether the engagement is an engineering risk assessment, a gap assessment against named requirements, independent assurance, or a combination with the responsibilities separated. The decision changes the evidence standard, the sampling and the words the report may use. Name the intended recipients and who may receive the technical appendices. If the assessment team or its firm designed, installed or operates any of the controls in scope, disclose that relationship before any part of the work is described 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 the identity, DNS, time, virtualization, telecommunications and backup dependencies whose failure could affect the process, because the services that can actually take the process down belong in the record alongside the controller. Identify shared corporate services and third party interfaces explicitly, and record that naming them in the boundary leaves test permission with the activity permits. For each legal entity record the physical address, owner, operator, sector, production or service function, permits, regulators, contracts, insurer conditions and public body status. For distributed assets list every other state, local authority and control center involved.

Define exclusions

Document every excluded safety system, vendor appliance held outside the access arrangements, firmware past vendor support, protocol held back from testing and record awaiting production, and state in one sentence how each exclusion shapes the conclusion. An excluded critical dependency stays in the report as a

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

visible scope decision that the sponsor accepted. Holding the asset count steady from scoping to report keeps the scope matched to the estate rather than to what was convenient to examine.

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 the open items. Each signature is dated and kept with the scope record, and approval is that written signature, given by each of these people in turn.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

Roles and decision authority

Assign people and alternates before work starts, and record them where the field team can find them during an outage. Small organizations may combine roles, but three authorities stay explicit no matter how small the team: who authorizes operating activity, who reviews evidence, and who accepts residual risk.

Role	Decision or work owned
Sponsor or CISO	Approves the business objective, the resources and the reporting audience. Accepts residual business risk within delegated authority and records that acceptance in writing.
Operating owner and engineering authority	Approve process boundaries, safe state and production methods. The control center and the responsible electrical authority retain switching, dispatch and protection authority.
Compliance and legal owners	Resolve the applicable instruments, disclosure restrictions and incident reporting duties. Identify the responsible filing official and an alternate who can act in the official's absence.
Technical lead and field technician	Design the permitted method and collect traceable evidence. The technician works to the approved target list and the permitted tool settings, and the operating owner authorizes any active test.
Project manager	Sequences work, tracks evidence and approvals, protects operating windows, manages changes and closes acceptance records. Owns the open items register.
Evidence custodian and quality reviewer	Control evidence access, integrity, retention and the independent review of facts and conclusions. Record conflicts of interest and review exceptions.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

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

Project stages and acceptance

Plan by completed decisions and evidence rather than by a fixed number of days. Populate durations and staffing once site access, document availability and maintenance windows are known, and treat each stage's exit evidence as the gate for the next one.

Stage	Required exit evidence
1 Applicability and scope	Signed facility register, controlling instruments, exclusions and reporting scope. Every open legal question has an owner and a stated effect on the engagement.
2 Readiness	Approved evidence request, interview schedule, collection method, secure workspace, current backup evidence and operating contacts with alternates.
3 Examination	Asset and process records, reconciled diagrams, sampled control evidence and a dated account of what was examined and what was set aside, with the reason.
4 Authorized validation	Activity permits, baseline observations, test log, stop and recovery record and post work operating acceptance. Where validation was held back, the record states that decision and the reason for it.
5 Reporting and decisions	Reviewed findings, requirement mappings, limitations, corrective owners, funding decisions and a residual risk record signed by the person entitled to accept it.
6 Verification and handover	Retest evidence, recurring review schedule, retained records, lessons and a signed handover. A recommendation closes when it is verified or formally dispositioned.

Sources: NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

Applicability and obligation records

Use one row per obligation. A single facility can carry several reporting clocks, several evidence packages and several responsible officials for the same event, and a register that gives each its own row keeps every deadline in view.

Make a defensible decision

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

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

Separate obligation types

Federal requirements, state utility orders, public agency standards, local permits and contracts overlap on the same equipment. Use the fifty state companion to select additional checks, and confirm municipal, county, tribal or territorial authority where it is relevant. Municipal ownership can change utility jurisdiction and public entity duties, and a federal obligation that independently applies stays in force alongside them.

Preserve the reasoning

The compliance owner signs the decision date and the next review trigger. Save the instrument and its source URL in controlled records and name the person who will watch for amendments. For an incident clock record the trigger event, the start timestamp with its time zone, the deadline rule, the recipient, the permitted channel, the responsible official and the receipt. The auditor's first question about any applicability decision is why it was made and by whom, and this record is the only acceptable answer.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), CIRCIA public rulemaking notice (F05), Cybersecurity Resource Center (F09)

Bulk power applicability

NERC CIP applicability begins with the registered function, the facilities, the systems and the applicable standard. It follows from those registration facts rather than from the word energy in a company description, and the applicability record is the document an auditor reads before any control evidence.

Freeze the applicability record

Obtain the entity registration, the functional roles, the relevant facilities, the BES Cyber System categorization, the asset ownership and the accountable compliance owner, each as a dated export or signed record rather than as a verbal confirmation. Identify the applicable exceptions and the system boundaries. Record the exact requirement and version in force for the assessment period rather than a generic CIP compliant label, because every finding will be measured against that exact requirement.

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, the implementation plan, the enforcement date and the transitional scope together in one record, and apply a newly approved revision from its effective date, testing against the edition that binds the entity for the review period.

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 each overlap at the specific system boundary with the responsible compliance owners, and record which regime governs each shared network segment.

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

Evidence accepted

The compliance owner signs the registration, the categorization and the requirement matrix. Include a controlled copy of each applicable instrument and a watchlist for future changes. A complete CIP compliance conclusion for an item rests on the current standard and a settled boundary, and the report states plainly which items are waiting on either.

Sources: Critical Infrastructure Protection reliability standards register (P01), New bulk power reliability safeguards (P02), Reliability standards and US effective date resources (P03), Nuclear cybersecurity (P05)

CIP evidence workstreams

Use these rows as candidate evidence workstreams. Each one requires the applicable requirement, edition, system and population to be established first, and each names the kind of evidence the assessment will ask the compliance program to produce.

Workstream	Evidence and examination
Categorization and governance	CIP-002 and CIP-003. Review the categorization rationale, the responsible roles, the policy approval and the applicable low impact controls.
People and electronic access	CIP-004 and CIP-005 where applicable. Examine authorization, training, remote access, electronic boundaries and revocation samples drawn from the actual population and period. Keep the exact population and assessment period in the record.
Physical and system controls	CIP-006 and CIP-007 where applicable. Review access records, approved system security processes and evidence that they operated during the period. Identify legacy limitations and the exceptions that cover them.
Incident and recovery plans	CIP-008 and CIP-009 where applicable. Review the plan version, exercise or test evidence, roles, results and corrective work.
Configuration and vulnerability work	CIP-010 where applicable. Link baseline, change and assessment evidence to the named system and requirement.
Information, supplier and future monitoring scope	CIP-011, CIP-013 and other applicable standards. Review protected information handling and supplier risk evidence. Track CIP-015 and other future obligations on their own rows, and set each one's enforcement date and system scope from the confirmed implementation plan.

Sources: Critical Infrastructure Protection reliability standards register (P01), Reliability standards and US effective date resources (P03)

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

Distribution DER and state utility programs

State oversight, public power governance and contracts carry the duties for scoped systems outside NERC CIP applicability. A distribution utility outside the NERC registry answers to a commission, a board and its contracts, and those documents define the assessment criteria.

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, and keep the actual documents in the controlled record.

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. Delaware describes annual Class A utility cyber filings. Tennessee and other states have separate utility programs that need current scope and filing checks, and the fifty state companion routes you to the selected source for each.

Use guidance appropriately

The NARUC and DOE distribution baselines are guidance, and they can support a gap assessment when the owner agrees to them as criteria. Identify any commission order or contract that adopts them and use the adopted edition, and record in the report that the baseline is an agreed criterion rather than a legal requirement.

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, because fleet management platforms routinely can.

Sources: Electric distribution cybersecurity baselines (P06), Utility IT cybersecurity regulations announcement (P07), Delaware PSC cybersecurity requirements (S08), Tennessee rule filing 06-31-23 (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. The examination moves from the control room outward, and every step is validated by the people who operate that layer.

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

Control centers

Reconcile the EMS and DMS services, the engineering and operator roles, the communications paths, the identity dependencies and the recovery procedures against the running system. Review the approved handling of telemetry failures and inconsistent data. Examine records that show a critical event actually reaching the responsible operator, such as alarm logs matched against the operator's acknowledgment, rather than a description of the alarm philosophy.

Protection and substations

Identify the gateways, the remote access, the relay engineering tools, the time synchronization and the responsible protection engineer. Review the approved settings management and the change evidence, including the settings file repository and its comparison against the relay.

Plant and station services

Trace the DCS, balance of plant systems, fuel, cooling, backup power and telecommunications dependencies appropriate to the facility. Identify nuclear, pipeline or other separately regulated boundaries that share the site. Record which specialist must review each high consequence pathway, and have the protection or plant engineer sign each pathway alongside the cyber assessor.

Deliverable Review and Acceptance Criteria

The control center and engineering authorities validate the diagram and the consequence assumptions. Preserve discrepancies and access limitations in the record. A laboratory relay or representative controller test identifies the firmware, configuration and topology differences from the installed equipment before any conclusion is drawn from it.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), Critical Infrastructure Protection reliability standards register (P01), Nuclear cybersecurity (P05), ICSSIM: A framework for building industrial control systems security testbeds (R03)

Power incident and recovery exercise

This fictional exercise tests whether the people who would make the decisions can find the records they need.

Scenario

An engineering support account appears in a remote access record at an unexpected time. A station reports intermittent visibility. Whether the protection configuration has changed is the open question.

Test the operating response

The dispatcher determines the operating response and the required communications. The technical lead identifies the current evidence, the clock differences between the access platform and the station, and what the evidence gathered so far supports. The protection engineer identifies how configuration integrity will be

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

established through approved evidence rather than by connecting to the relay.

Test the reporting decision

The compliance owner evaluates the applicable NERC incident definitions, the DOE-417 categories, the state utility reports, any nuclear or pipeline obligations and the contractual notices. The exercise record lists each clock and who started it.

Test restoration dependencies

Locate the approved recovery sequence, the trusted configurations, the engineering tools, the licenses, the spare equipment and the vendor support arrangements. Record which steps were discussed and which have prior test evidence. Assign corrective work for every dependency to be supplied and every assumption awaiting a test.

Sources: NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04), Critical Infrastructure Protection reliability standards register (P01), Electric Emergency Incident and Disturbance Report (P04), Nuclear cybersecurity (P05)

Power reporting and recurring calendar

Use the applicable instrument for each event and each control population. A calendar built from the entity's own states and registered functions carries every duty that attaches to them, row by row.

Calendar item	Record to maintain
NERC requirement schedule	Current standard edition, requirement and part, system population, interval, transition rule, responsible owner and evidence period for every applicable requirement.
State utility program	Commission rule or order, entity classification, annual filing or exercise requirements, confidentiality procedure and the submission receipt.
DOE-417 and other incident reporting	Event category, threshold, clock from the 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: Critical Infrastructure Protection reliability standards register (P01), Reliability standards and US effective date resources (P03), Electric Emergency Incident and Disturbance Report (P04), Nuclear cybersecurity (P05), Pipeline Cybersecurity Mitigation Actions Contingency Planning and Testing (T03), Pipeline control room management (T05)

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

Document requests and interviews

Request existing records before anyone proposes a live connection. Most of what a competent OT assessment needs already exists in engineering, maintenance and identity systems, and asking for it first tells you how well the operator knows its own process before a single packet is observed.

Initial evidence request

Request the asset inventory, the approved network and process drawings, the process description, current configuration exports, the remote access arrangements, the account owner list, maintenance records, the backup inventory and the most recent 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 the change history for the period in scope. Give each request an identifier, a purpose, an expected owner, a time period, a format and a due date, and arrange a supervised on site review for any record that stays at the facility. Log each outstanding item together with its effect on the conclusion.

Interviews that test the record

Ask operations what happens when visibility, remote control, communications or a critical vendor service is lost, and listen for whether the answer names a procedure or a person. Ask engineering which installed details differ from the drawing; there are always some, and the honest list is the most useful document the assessment will receive. Ask the identity owner how vendor access is approved and revoked and request the last revocation as evidence. Ask the recovery owner for the record of the last actual restore rather than a description of the backup product.

Sampling

Define the control population and the sampling rationale before selecting items. Include the material differences in site function, equipment family, criticality, remote access and support arrangements so the sample represents the estate rather than the nearest site. A sample drawn across the estate speaks for the remote stations as well as the nearest one, and the report states in plain terms both the sample and the rest of the population.

Readiness evidence

Retain the request register, the interview notes with participants and dates, the source versions received, the missing item log and the agreed question list for the field visit. Before the visit the technical lead reads the notes once more to confirm that each interview statement is labelled as a statement and each tested fact as tested.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

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

Safe work and stop authority

The control center and the responsible electrical authority retain switching, dispatch and protection authority. These sentences are the operating rule for the entire engagement, and every member of the assessment team can repeat them from memory before the first site day.

Before connecting anything

Attend the operator's safety briefing and follow the site access, electrical, hazardous energy, confined space and other controls that the operator says apply. The operator determines which safety program governs, and electrical switching, confined space entry and plant permits stay with the operator's qualified personnel, whatever cyber credentials the assessor holds. Before any collection device is attached, verify the asset owner, the permitted access point, the device approval, its malware screening, the cable path and the isolation design. A mirror port or passive tap design can affect traffic handling, data exposure and network load, so its installation and its removal are both approved steps.

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 in the operator's own terms: unexpected alarms, impaired communications, controller health changes, operator concern or any departure from the approved method. The number that matters is the one the operator watches. Name who can stop work and who can authorize resumption. Any technician may call a safety stop. The operating owner directs the plant response, including any isolation, device reset or process restart, and the assessor follows that direction.

Record the stop and recovery

Log the time, the activity, the observed symptoms, the notifications made, the actions directed by operations and the restoration evidence. Preserve the available records alongside the safety response, which always comes first. Quarantine the activity permit while operations and the technical lead review the cause, then reauthorize the changed method for the remaining targets. A stop that is logged and reviewed is a mark of a controlled assessment, and the log shows a later reviewer how the team handled it.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), State Plans (F06)

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

Inventory and process dependencies

Build an inventory that explains how each asset supports generation, transmission, distribution, protection, dispatch, storage, gas operations and supporting station services. A working inventory reconciles IP address lists and passive discovery exports against the drawings and ties each entry to the process it supports.

Use existing evidence first

Reconcile the engineering inventories, configuration exports, approved drawings, maintenance records and supervised physical observation into one record. For each asset capture the identifier, function, location, owner, manufacturer, model, firmware or software version, support status, protocols, zone and recovery dependency. Mark each value as observed, taken from a configuration export, or supplied by a vendor or operator, because the three carry different weight and a reviewer will ask which one applies.

Trace the consequence

For each critical process trace the route from the operator interface and the control logic through communications to field equipment and the 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 the available protection or manual alternative, then write down what they said and who said it. Record protective functions separately from normal process control and document the dependencies on identity, time sources, licensing, cloud support, third party communications and engineering tools. A safety function counts as independent when engineering has shown you how it is isolated, whatever layer of the drawing it appears in.

Resolve discrepancies

Mark unidentified devices, duplicated identifiers, outdated drawings and vendor assets awaiting verification, and give each discrepancy to its owner to resolve. A system past vendor support needs a control and recovery decision, and any patch, scan or replacement during the assessment goes through the operator's change approval. Expect the first reconciliation to surface undocumented engineering laptops, dual homed workstations and vendor modems; those are findings, not embarrassments, and the inventory is where they are recorded.

Deliverable Review and Acceptance Criteria

The asset owner signs the scoped inventory and the dependency map. The report states the sources used, the collection date, the coverage achieved and every open high consequence dependency. Sensitive addressing and configuration detail belong in the controlled technical appendix, and the management report summarizes them.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), A survey of cyber security management in industrial control systems (R01), Threat modeling of industrial control systems: A systematic literature review (R02)

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

Network paths and remote access

Review every path by which a person, a service or an external system can reach the scoped process. A firewall diagram is a hypothesis that the examiner tests against the rule base, the routing and the actual sessions, and that comparison is where segmentation claims are confirmed or corrected.

Examine the intended boundary

Use dated configuration exports, rule bases, drawings and approved architecture records to identify the zones, conduits, remote entry points, jump services and management interfaces. For each material path record the source, the destination, the permitted service, the business purpose, the approver and the review date. Separate corporate identity, vendor support, telemetry, cloud management and emergency access into their own path records. Check whether access can be limited to named users and required assets, and whether it is reviewed, recorded and revoked. Examine an actual approval and an actual revocation from the period rather than the policy that describes them.

Examine the actual access process

Observe a supervised, approved support session or review the retained session records. Record how the user authenticated, how authorization was granted, who owns the account, whether the session was visible to operations, what constraints apply to shared accounts and how timeout and revocation behave. Where the desired mechanism sits better at an approved access gateway than on an installed controller, evaluate the controls there and say so in the finding. The examiner looks first at the usual weak points: a vendor tunnel that bypasses the jump host, a rule base with permit any entries left from commissioning, and a dual homed engineering workstation that joins two zones the drawing shows as separate.

Match each claim to its method

A configuration review identifies an allowed policy path, and a controlled connectivity check is a separate authorized activity with its own permit. A proposed segmentation improvement is recorded as a recommendation and moves forward as it is implemented and verified, and the report uses those three words, allowed, reachable and verified, with their distinct meanings.

Required records

Retain the approved path register, the source versions examined, the access samples, the exceptions and the method used. If ISA/IEC 62443 is contractual, obtain the licensed edition and the agreed assessment criteria, and measure any conformity claim against them. The publicly described zone and conduit approach is a design method, and a conformity or certification claim rests on the licensed edition.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), ISA/IEC 62443 Series of Standards (F08)

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

Accounts, legacy systems and suppliers

Start with the access needed to operate and recover the process, then identify the controls the installed system can actually support and the protections applied around it. Legacy equipment is assessed on the compensating controls around it, measured against what the installed system can support.

Accounts and authorization

Review named users, service accounts, vendor accounts and emergency credentials through approved exports of the identity directory, the local account stores on controllers and HMIs, and the vendor access platform. Verify owners, privileges, approval, periodic review and the revocation evidence for people who have left. Review how privileged access is separated from normal user activity. Record account names and roles. For every shared or embedded account document the technical limitation, the compensating controls, who knows the credential, how its use is supervised and logged, how access is removed when people leave and what change would reduce reliance on it. Most sites have a shared operator account with a password set at commissioning, and a well run site has the compensating controls around it written down and working.

Support and vulnerability decisions

Match versions and support status to vendor advisories using approved evidence. Separate a version match, a suspected vulnerability and a validated condition, and keep them separate in the finding register. A controller that answers a scan slowly is a reason to stop and review the scan plan. 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 own change process.

Supplier obligations

Review the supplier contracts for remote access, notification, vulnerability handling, evidence availability, subcontracting, licensing and exit support, and compare the paper to the observed practice. Identify each contractual promise that needs evidence behind it and each dependency that needs a named owner. Include a supplier contact and an escalation alternate in the operating handover so the operator can reach support directly during an incident.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), ISA/IEC 62443 Series of Standards (F08)

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

Monitoring, time and evidence handling

Establish whether the available records can answer who accessed what, when, through which path and with what effect. Record time offsets as found and leave the production clocks as they are, so the evidence keeps its original timing.

Collect a usable record

Identify the event sources, the collection routes, the retention settings, the access restrictions and the review responsibility for each. Include the jump host, authentication, firewall, engineering workstation and system records relevant to the scoped process. Verify that a small authorized event sample actually appears at the intended collection point, because the collection point's own records are where the examiner confirms what was received last month. Record the time zone, the clock source, the observed offset and the coverage periods for each source. If clocks disagree, preserve the original timestamps and document the translation used in analysis. An absent event is checked against collection coverage before it is read as inactivity, and the report states which reading the evidence supports.

Evidence integrity

Assign each item a stable evidence identifier and record its 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 every transformation and redaction. This is the discipline that lets a finding survive challenge from a vendor, a regulator or the other side in a dispute, and it costs minutes at collection time against hours of argument later.

Sensitive information

Have the compliance owner classify customer information, engineering records and any SSI, CEII, CUI or protected public records before collection begins, and apply the handling rules that actually attach to each class.

Deliverable Review and Acceptance Criteria

The custodian verifies access, recoverability and retention against the applicable instrument or the agreed contract. Preserve incident records and any legal hold independently of the normal assessment deletion date.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04)

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

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. A successful backup job records that a file was written, and recovery is tested through a representative restore.

Define the restoration objective

Ask operations to identify the minimum service, the safe process condition, the restoration sequence and the maximum tolerable interruption. Record the chosen recovery objectives, their owner and the evidence that supports their feasibility.

Examine recovery dependencies

Identify the controller and server configurations, engineering projects, firmware, software, licenses, keys held in controlled storage, approved hardware, spare components and vendor support that a restoration needs. Confirm where a clean engineering station and trusted installation media are kept for use during an incident, and whether a copy of the engineering software sits apart from the workstation an attacker would reach first. Review backup isolation, access, integrity checks and the evidence of a representative restore. A production controller upload, download or failover is a separately approved activity, and an isolated or representative system is the preferred setting whenever production is better left running.

Exercise and validate

Use a scenario that removes a material dependency. Record which recovery steps were discussed, which were demonstrated in a representative environment and which were performed in production under approval. Document the differences between the test environment and the installed system. A tabletop exercise tests the decision process, a technical restore tests the recovery itself, and the report keeps the two distinct.

Closure evidence

Retain the recovery procedure version, the scenario, the approvals, the result, the elapsed time where it was measured, the open dependencies and the corrective owner. Operations accepts the restored state. Assumptions awaiting a test stay explicit in the report and in the recurring program.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04), ICSSIM: A framework for building industrial control systems security testbeds (R03)

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

Authorization for active validation

Active validation enters the work when a controlling requirement or the agreed scope calls for it and an acceptable method has been authorized. A contractual requirement to test is met with a safe operating method, written down by the assessor before the work runs.

Write an activity permit

Identify the exact targets, the system owner, the purpose, the tool and its version, the commands or test functions, the allowed traffic behavior, the exclusions, the operating window and the collection location. Include vendor restrictions, communications arrangements, recovery support and the evidence to retain. Approve the method for the installed firmware and configuration rather than for a similar laboratory device, because controllers of the same model and different firmware behave differently under the same probe.

Choose the least disruptive evidence

Consider configuration examination, supervised control demonstration, existing logs and validation in a representative environment before any production probe. Record which requirement each method addresses and what it shows. Peer reviewed testbed research helps explain test design.

Confirm readiness at the point of work

Operations confirms the process condition and the baseline indicators. The technical lead confirms the approved tool settings and targets. The evidence custodian confirms that recording is running. The project manager verifies that the authorization is current and that the named stop authority is reachable by a channel that has been tested that day. Each of those is a separate activity with its own method, environment and approval.

Close the permit

Record the start and end times, the targets actually reached, deviations, stops, observations and the operating owner's acceptance. Revoke temporary access and remove approved collection equipment under the agreed procedure. Keep the original permit and the test record linked to every finding that relied on them.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), ICSSIM: A framework for building industrial control systems security testbeds (R03)

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

Writing findings that can be audited

A finding shows the condition, its evidence, the criterion it was measured against and its significance for the process. Observed facts and possible operating consequences are kept in separate sentences, so a reviewer can weigh each one on its own evidence.

Minimum finding record

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

Use precise status

Use Observed when the available evidence establishes a condition, and Suspected or Unresolved while corroboration is in progress. Record recommendation, implementation and verification as three separate states. A screenshot of a changed configuration supports implementation.

Prioritize consequence and uncertainty

Evaluate the potential effects on generation, transmission, distribution, protection, dispatch, storage, gas operations and supporting station services, the exposure paths, the existing safeguards, the recovery limits and the 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, and have engineering review the pathway before it is presented as fact. A CVSS score describes a software vulnerability, and plant risk comes from the organization's own method. Record that risk method and the acceptance authority, and build the plant risk rating from it so its precision matches the evidence.

Resolve challenge

Give the operating owner a documented opportunity to correct asset facts, add safeguards the report should credit and flag remediation proposals that need a safer approach. Retain the challenge, the additional evidence, the reviewer's decision and the revised wording. A disagreement closes when the record shows how it was resolved, whatever the delivery date of the report.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), A survey of cyber security management in industrial control systems (R01), Threat modeling of industrial control systems: A systematic literature review (R02)

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

Corrective work and management reporting

The assessment ends with decisions an owner can implement and a reviewer can verify. A corrective plan puts the vulnerabilities into an operating sequence, and that sequence turns a scan export into work the plant can schedule.

Plan the work

For each accepted finding identify the owner, the dependency, the required design or procurement, the change approval, the maintenance window, the recovery support, the target date and the verification evidence. Identify an interim control where the final fix takes longer, and keep the label Deferred on a deferred action through to its implementation. Sequence actions by operating consequence and dependency: an access boundary may need a maintained jump host, named accounts and supplier support in place before a legacy controller can be isolated, and applying fixes in that order keeps the operator supported through the next outage. Verify that each proposed change preserves emergency operation and recovery.

Report to leadership

Provide a concise operating risk summary, the most consequential open issues, the funding or outage decisions required, the affected services and the scope boundaries of the assessment. Show the remaining work and who may accept the residual risk. Confidential addressing and detailed weaknesses stay in the restricted appendix.

Report to technical owners

Provide enough evidence and context to reproduce each observation using the approved method. Identify configuration versions, the affected boundary, exceptions and the exact acceptance criteria for closure.

Regulatory conclusion

State the obligations actually assessed, with their versions, the facility scope, the sample and the dates, and list separately the requirements that sit outside this assessment or await demonstration.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

Verification closure and recurring work

Close an action against the evidence defined when the finding was written. A management assertion, a purchase order or a completed ticket is the reason to schedule verification, and the verification produces the control result.

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

Verification procedure

The reviewer checks that the 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 state whether the result establishes design, implementation or operating effectiveness, because those are three different claims.

Evidence Handover and Chain of Custody Transfer

Return the current inventory, dependency map, control and finding register, activity permits, evidence index, operating procedures, supplier contacts and training record to the designated owners. Check that authorized staff can retrieve those records during an outage, including one that takes down the corporate document system. Remove temporary access under the agreed change record and confirm the removal.

Recurring triggers

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

Final acceptance

The operating owner accepts the process condition and the handover. The technical reviewer signs the evidence based conclusions. The compliance owner approves the requirement mapping and the remaining legal questions. The sponsor records the funding and residual risk decisions. The project manager closes each deliverable as it meets those acceptance criteria, and the closure record names each person and date.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04)

Facility and applicability worksheet

Complete one worksheet for each legal entity, facility and distinct regulatory boundary, and keep the source records in controlled storage. The worksheet is the index an auditor reads first, so every field points to a record that exists.

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

Evidentiary Record Fields

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 begins. This worksheet records that permission.

Evidentiary Record Fields

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, preserve the source times and state the method and its scope, so any qualified reviewer can reproduce the finding from the record.

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

Evidentiary Record Fields

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 as three separate states with their own dates and evidence. Record the remaining risk and name the person authorized to accept it.

Evidentiary Record Fields

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.

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

Term	Meaning in this pack
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 marks a fact or authority awaiting confirmation, and it is a separate status from Not applicable.

Sources F01 to R03, federal guidance and peer reviewed research

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 was released as an initial public draft on September 21, 2026, so Revision 3 remains the final baseline.

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, while current law and any effectiveness figures come from the primary instruments.

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, and each plant assessment is validated on its own evidence.

R03 ICSSIM A framework for building industrial control systems security testbeds

Computers in Industry. Peer reviewed research. Volume 148 June 2023 article 103906.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-82 Rev. 4 initial public draft, Guide to Operational Technology (OT) Security (F02), A survey of cyber security management in industrial control systems (R01), Threat modeling of industrial control systems: A systematic

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

literature review (R02), ICSSIM: A framework for building industrial control systems security testbeds (R03)

Sources F03 to P02, federal guidance and power and energy instruments

F03 Technical Guide to Information Security Testing and Assessment

NIST. Final guidance. Assessment planning and rules of engagement. Apply OT operating constraints.

F05 CIRCIA public rulemaking notice

CISA and Federal Register. Rulemaking record. 2026 notice referring to the proposed rule and further town halls. The CIRCIA final rule has been under review at the Office of Management and Budget since October 1, 2026 and is pending, so confirm its status in the Federal Register before setting a reporting clock.

F09 Cybersecurity Resource Center

New York DFS. Agency implementation source. 23 NYCRR Part 500 covered entity scope. Covered entity status turns on the definition in 23 NYCRR Part 500, so an industrial operator in New York is checked against that definition.

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, which set the enforcement dates for each approval.

Sources: NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), CIRCIA public rulemaking notice (F05), Cybersecurity Resource Center (F09), Critical Infrastructure Protection reliability standards register (P01), New bulk power reliability safeguards (P02)

Sources P03 to S08, power and energy

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

instruments and state authorities

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. Guidance; its binding force comes through state adoption or contract incorporation, so identify each.

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, reviewed October 16, 2026.

Sources: Reliability standards and US effective date resources (P03), Nuclear cybersecurity (P05), Electric distribution cybersecurity baselines (P06), Utility IT cybersecurity regulations announcement (P07), Delaware PSC cybersecurity requirements (S08)

Sources S42 to T05: Power, Transportation and State Authorities

S42 Tennessee selected authority

Tennessee Secretary of State. Filed utility rule. Selected state authority and applicability, reviewed 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, since each event category carries its own clock.

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

T03 Pipeline Cybersecurity Mitigation Actions Contingency Planning and Testing

TSA. Security directive. Security Directive Pipeline-2021-02G, effective May 3, 2026 through May 2, 2027, supersedes Pipeline-2021-02F, and Pipeline-2021-01G, issued January 15, 2026, carries the reporting requirements. Obtain the applicability notice and approved plan 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: Tennessee rule filing 06-31-23 (S42), NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04), Electric Emergency Incident and Disturbance Report (P04), Pipeline Cybersecurity Mitigation Actions Contingency Planning and Testing (T03), Pipeline control room management (T05)

Sources F06 to F08, federal guidance

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. The normative texts are licensed from ISA and IEC, and a conformity or security level claim rests on the licensed edition the organization holds.

Sources: State Plans (F06), ISA/IEC 62443 Series of Standards (F08)

READY TO PLAN THE ASSESSMENT?

Plan the Assessment With Examiners Who Leave Switching to Operators

The manual gives you the applicability record, the evidence workstreams and the field permits. Global Digital Forensics supplies the examiners who carry them into the control center and the substation: court tested forensic specialists who have served businesses since 1992, who gather the evidence an applicable NERC CIP requirement or a state program will ask for, who authorize every active step with the control center by name and who write findings a compliance owner, a protection engineer or a board can follow. Tell us about the registered functions, the facilities and the programs in play, and we will scope the work with your operating leads. The first consultation is free.

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

Web Addresses for the Sources Cited

1. NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security: https://csrc.nist.gov/pubs/sp/800/82/r3/final
2. NIST SP 800-82 Rev. 4 initial public draft, Guide to Operational Technology (OT) Security: https://csrc.nist.gov/pubs/sp/800/82/r4/ipd
3. A survey of cyber security management in industrial control systems: https://doi.org/10.1016/j.ijcip.2015.02.002
4. Threat modeling of industrial control systems: A systematic literature review: https://doi.org/10.1016/j.cose.2023.103543
5. ICSSIM: A framework for building industrial control systems security testbeds: https://doi.org/10.1016/j.compind.2023.103906
6. NIST SP 800-115, Technical Guide to Information Security Testing and Assessment: https://csrc.nist.gov/pubs/sp/800/115/final
7. CIRCIA public rulemaking notice: https://public-inspection.federalregister.gov/2026-10417.pdf
8. Cybersecurity Resource Center: https://www.dfs.ny.gov/industry_guidance/cybersecurity
9. Critical Infrastructure Protection reliability standards register: https://www.nerc.com/standards/reliability-standards/cip
10. New bulk power reliability safeguards: https://www.ferc.gov/news-events/news/ferc-action-new-reliability-safeguards-american-power-grid
11. Reliability standards and US effective date resources: https://www.nerc.com/standards/reliability-standards
12. Nuclear cybersecurity: https://www.nrc.gov/facilities-safety/cybersecurity
13. Electric distribution cybersecurity baselines: https://pubs.naruc.org/pub/364B7A14-D21C-D2DF-BB6B-FFF3F93E1D51
14. Utility IT cybersecurity regulations announcement: https://dps.ny.gov/node/29056
15. Delaware PSC cybersecurity requirements: https://depsc.delaware.gov/cybersecurity/
16. Tennessee rule filing 06-31-23: https://publications.tnsosfiles.com/rules_filings/06-31-23.pdf
17. NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: https://csrc.nist.gov/pubs/sp/800/61/r3/final
18. Electric Emergency Incident and Disturbance Report: https://doe417.energy.gov/
19. Pipeline Cybersecurity Mitigation Actions Contingency Planning and Testing: https://www.tsa.gov/sites/default/files/signed_security_directive_pipeline-2021-02g_and_transmittal_memo_508c.pdf
20. Pipeline control room management: https://www.phmsa.dot.gov/pipeline/control-room-management/control-room-management
21. State Plans: https://www.osha.gov/stateplans/
22. ISA/IEC 62443 Series of Standards: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

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