Transportation OT assessment planning pack

Planning edition October 16, 2026

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

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

Purpose

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

Working records

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

Facility adoption

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

Contents

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

3 Planning scope and research basis
4 Using the corrected workbook edition
5 Using this planning pack
6 Decisions before mobilization
7 Roles and decision authority
8 Project stages and acceptance
9 Applicability and obligation records
10 Transportation mode and operator boundaries
11 Maritime obligations and milestones
12 Maritime recurring work register
13 Rail and transit assessment planning
14 Pipeline and energy transport planning
15 Aviation ports and roadway field boundaries
16 Transportation exercise and handover
17 Document requests and interviews
18 Safe work and stop authority
19 Inventory and process dependencies
20 Network paths and remote access
21 Accounts legacy systems and suppliers
22 Monitoring time and evidence handling
23 Recovery and continuity evidence
24 Authorization for active validation
25 Writing findings that can be audited
26 Corrective work and management reporting
27 Verification closure and recurring work
28 Facility and applicability worksheet
29 Field activity authorization worksheet
30 Evidence and finding worksheet
31 Corrective action and acceptance worksheet
32 Terms used in the planning records
33 Sources and instrument status
34 Sources and instrument status
35 Sources and instrument status
36 Sources and instrument status
37 Sources and instrument status

Planning scope and research basis

This pack supports a controlled assessment of rail and transit movement, road traffic management, port and terminal operations, aviation support and pipeline control in the United States. Use the companion volume to screen all 50 states and resolve the actual local and facility requirements.

What the assessment produces

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

Research cutoff

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

Open applicability

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

Adoption and review

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

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

Using the corrected workbook edition

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

Before execution

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

Open and incomplete decisions

The open count includes blanks, invalid decision text and resolved selections missing required record fields. Fields present still requires qualified review. Actual approvals remain uncompleted until the responsible people review the work.

Scope and authority

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

Source access and revision

Sources list retrieval status and available snapshot hashes. A restricted URL is not proof that a duty does not exist. Edition record tracks actual project revisions and reviews. Retain the previous edition and do not treat a template publication as a personal technical or legal approval.

Sources: F01, F03.

Using this planning pack

Use this pack to organize an assessment of rail and transit movement, road traffic management, port and terminal operations, aviation support and pipeline control. Start with the legal and operating boundary. Select evidence and methods only after the people responsible for the process agree what may be examined.

First use

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

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

Reading the evidence

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

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

Before signing an assessment conclusion

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

Sources: F01, F03.

Decisions before mobilization

Split the engagement by mode and regulatory boundary. Surface rail, urban transit, roads, maritime facilities, vessels, airports, aircraft and pipelines require different applicability and evidence decisions.

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 rail signaling interfaces, traction-power SCADA, tunnel systems, traffic controllers, terminal cranes, access systems, airport operational support, pipeline SCADA and remote control sites. Include supporting identity, DNS, time, virtualization, telecommunications and backup dependencies when their failure could affect the process. Identify shared corporate services and third-party interfaces without silently expanding test permission.

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

Define exclusions

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

Release decision

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

Sources: F01, F03.

Roles and decision authority

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

Role	Decision or work owned
Sponsor or CISO	Approves business objective, resources and reporting audience. Accepts residual business risk only within delegated authority.
Operating owner and engineering authority	Approve process boundaries, safe state and production methods. The dispatcher, control-room supervisor, port or terminal authority, airport operations lead or pipeline controller retains operating authority. Do not test movement authority, signaling, runway lighting, emergency ventilation, cranes or pipeline commands in live service without the appropriate approved operating procedure.
Compliance owner and counsel	Resolve applicable instruments, disclosure restrictions and incident-reporting duties. Identify the responsible filing official and alternate.
Technical lead and field technician	Design the permitted method and collect traceable evidence. A technician cannot expand the target list or authorize an active test.
Project manager	Sequences work, tracks evidence and approvals, protects operating windows, manages changes and closes acceptance records.
Evidence custodian and quality reviewer	Control evidence access, integrity, retention and independent review of facts and conclusions. Record conflicts and review exceptions.

Sources: F01, F03.

Project stages and acceptance

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

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

Sources: F03.

Applicability and obligation records

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

Make a defensible decision

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

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

Separate obligation types

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

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

Preserve the reasoning

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

Sources: F01, F05, F09.

Transportation mode and operator boundaries

Separate each mode, operator and approved security or safety program before applying an assessment checklist.

Mode	Authority and decision needed
Freight and passenger rail	Determine the carrier and whether a current TSA directive or security program applies. Obtain the issued instrument, notice, approved implementation plan and assessment program.
Urban transit	Determine FTA assistance, rail-transit status, State Safety Oversight and applicable TSA coverage. FTA identifies a cybersecurity planning certification under 49 USC 5323 v for covered rail transit operators.
Roads tunnels and traffic management	Identify state/local ownership, public-agency cyber policies, contracts, tunnel safety programs and operator procedures. No uniform federal annual traffic-controller cyber assessment duty was established here.
Maritime facilities vessels and OCS	Determine whether the owner/operator is required to have a security plan under 33 CFR Parts 104, 105 or 106. Apply the relevant 101 Subpart F provisions and current approval or waiver conditions.
Airports and aircraft operators	Obtain the current TSA-approved security program and amendments and the relevant FAA/airport operating constraints. Public summaries do not provide a complete clause-level cybersecurity assessment basis.
Hazardous liquid natural gas and LNG	Determine current TSA notification/directive coverage, PHMSA SCADA control-room rules and state pipeline authority. Record overlapping operator and system boundaries.

Sources: T01, T03, T04, T05, T06, T07, T08, T09.

Maritime obligations and milestones

33 CFR 101 Subpart F applies to specified owners and operators required to have security plans under 33 CFR Parts 104, 105 and 106. Do not assign it to every waterfront facility without checking that trigger.

Compliance timing

The final rule became effective July 16 2025. Coast Guard implementation information identifies January 12 2026 for the initial general training milestone and annual recurrence. July 16 2027 is the principal milestone for designation of the Cybersecurity Officer, completion of the Cybersecurity Assessment and submission of the Cybersecurity Plan for approval. Check later amendments, waivers and operator-specific conditions.

Assessment and plan evidence

Establish the vessel/facility scope, IT/OT inventory, critical functions, vulnerabilities, existing safeguards and remedial measures. The annual assessment and plan-maintenance program must link to a designated CySO and controlled records. Do not substitute a generic IT questionnaire for the required operational scope.

Testing and exercises

The final rule provides for penetration testing in conjunction with Cybersecurity Plan renewal under 101.650(e)(2), at least two drills each calendar year, and an exercise each calendar year with no more than 18 months between exercises. Check the precise applicable clauses, compliance schedule and approved alternatives before scheduling.

A penetration-testing obligation is not permission for unsafe production exploitation. Agree the targets, method, operator safeguards and any regulatory treatment of constraints before work. Keep drill, exercise, assessment, audit and penetration-test records distinct.

Handling

Determine SSI handling and approval channels for the actual records. Keep security plans and detailed vulnerabilities within authorized systems and recipients. The relevant Coast Guard approval or receipt is separate from assessor report delivery.

Sources: T01, T02.

Maritime recurring work register

The CySO assigns owners and retains evidence for separate obligations. Populate actual completion dates and apply the relevant compliance schedule, approval conditions and exceptions.

Workstream	Calendar and acceptance record
Assessment and plan audit	After the initial assessment, assess annually and sooner on ownership changes under 101.650(e)(1). The CySO also ensures annual and triggered plan audits under 101.630(f), with qualified independent auditors and required amendment follow-up. Retain scope, results and corrective decisions.
Personnel training	General and key-personnel training recur annually, with the initial milestone January 12 2026. New personnel train within five days of system access and no later than 30 days after hiring. Record the relevant OT topics and any authorized monitored-access arrangement.
Drills and exercises	Track at least two drills each calendar year and one exercise each calendar year, with at most 18 months between exercises. Keep participants, scenario, findings and correction records.
Penetration testing	Link the required test to Cybersecurity Plan renewal under 101.650(e)(2). Do not infer an initial-submission trigger. Retain approved targets, safe method, constraints, results and correction evidence.
Records and amendments	Section 101.640 routes records to 104.235, 105.225 or 106.230. Verify the applicable retention and secure access. Preserve required approvals and plan amendments separately from the assessment report.

Sources: T01, T10.

Rail and transit assessment planning

Separate current issued TSA obligations, grant-related duties and operational safety programs.

Obtain current instruments

The public rail directive 1580/82-2022-01D retrieved in this research expired May 2 2026. A replacement or extension was not authenticated. Treat that copy as historical. Obtain the operator's current directive and applicability notice through the designated security official. Protect SSI where applicable.

Build the evidence boundary

Map the operator's approved cybersecurity implementation and assessment arrangements to the actual systems. Include dispatch, traction power, wayside interfaces, tunnel ventilation, access systems and supporting communications when they are within scope. Identify third-party and shared-facility responsibilities.

FTA and state safety oversight

FTA identifies cybersecurity planning certification as a condition of assistance for covered rail transit operators under 49 USC 5323 v. Obtain FY2026 certifications and the actual award conditions. Separately identify 49 CFR Part 673 safety-plan and State Safety Oversight responsibilities. A safety-plan certification is not proof that a cyber control was tested.

Field method

Use approved diagrams, configuration records, access samples and event records first. Movement authority, signaling, traction power and emergency ventilation tests require the proper operating and engineering authorities. Do not inject traffic or test a failover against live signaling under a generic IT authorization.

Sources: F01, T04, T06, T07, T08.

Pipeline and energy transport planning

TSA cybersecurity instruments and PHMSA control-room safety rules can apply to the same operator for different purposes.

TSA applicability

Obtain the current directive, notice and approved operator plans. The public Pipeline-2021-02F copy retrieved here expired May 2 2026. A later instrument or extension was not authenticated. Do not issue a current compliance conclusion or assign an old reporting clock solely from that copy.

PHMSA control room boundary

Identify whether controllers in a control room monitor and control pipeline facilities through SCADA within 49 CFR 192.631 or 195.446 scope. Review the applicable control-room procedures, alarm management, point-to-point information validation, change management, training and operating records using the current rule and operator program.

Evidence and field work

Trace control and telemetry, communications, leak-detection interfaces, engineering access and vendor dependencies. Review authoritative configuration and alarm records with the control-room supervisor. Do not change pressure/flow commands, alarm thresholds or communications to demonstrate a cyber finding.

Overlap and reports

Record federal pipeline-safety, TSA, state pipeline, environmental and contractual notification criteria separately. Capture the actual event facts and awareness timestamps. A cyber report does not substitute for a release or safety report, and safe plant response takes precedence over evidence collection.

Sources: F01, T03, T05, F07.

Aviation ports and roadway field boundaries

These environments share technologies but have different operating authorities. Divide the work rather than using one approval for the entire campus or transport network.

Aviation

Distinguish airport enterprise IT, baggage/fuel/building systems, airfield operational systems, air traffic systems and aircraft. Obtain the operator's current security program and applicable amendments. Aircraft airworthiness and approved maintenance or modification procedures require the responsible aviation specialist. This pack does not establish aircraft product conformity.

Ports and terminal interfaces

Determine facility and vessel responsibilities, tenant connections, crane controls, cargo systems, reefer monitoring, access, shore services and third-party remote support. Link the boundary to the MTSA plan and current CySO. Tenant or lease obligations can supplement federal scope without changing the federal applicability test.

Road traffic and tunnels

Record state or local ownership, DOT or municipal contracts, communications providers, traffic control, tunnel ventilation, emergency power and recovery dependencies. Identify public-agency incident rules and local operating plans. No nationwide cyber audit interval for all traffic controllers was established.

Acceptance

Each responsible operator signs the boundary and permitted method. A port-wide corporate approval does not automatically authorize work on a vessel, aircraft, rail signaling system or separately owned tenant equipment. Unresolved ownership or operational authority stops the affected activity.

Sources: F01, T01, T08, T09.

Transportation exercise and handover

Use one scenario per mode and a separate coordination scenario for shared dependencies. The following scenario is fictional.

Scenario

Remote vendor access is suspected of compromise at a shared communications service. One operator reports loss of visibility while another still appears normal. It is unclear which interfaces share an identity or management path.

Operational decisions

Ask each operator to establish its safe response, service restrictions and decision authority. Ask the technical lead to identify the shared dependency and the limits of the evidence. Ask the project manager to account for tenants, contractors and cross-state assets without expanding test permission.

Reporting decisions

Have the responsible officials evaluate current TSA instruments, Coast Guard reporting, FTA/State Safety Oversight, PHMSA, state/local public-entity and contract duties as applicable. If a controlled directive is missing, record the missing instrument and escalation rather than inventing its deadline.

Closure

Record tested communications, identified delays, unavailable records, actions, owners and review dates. Reconcile any mode-specific safety acceptance, security-plan amendment or regulator receipt needed before return to service. A workshop does not prove technical restoration or regulator acceptance.

Sources: F04, T01, T03, T04, T05, T06, T08, T09.

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 rail signaling interfaces, traction-power SCADA, tunnel systems, traffic controllers, terminal cranes, access systems, airport operational support, pipeline SCADA and remote control sites. Ask for the applicable regulatory assessments, prior findings and change history.

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

Interviews that test the record

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

Sampling

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

Readiness evidence

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

Sources: F01, F03.

Safe work and stop authority

The dispatcher, control-room supervisor, port or terminal authority, airport operations lead or pipeline controller retains operating authority. Do not test movement authority, signaling, runway lighting, emergency ventilation, cranes or pipeline commands in live service without the appropriate approved operating procedure.

Before connecting anything

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

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

Define measurable stop conditions

Operations defines the baseline process indicators and limits appropriate to rail and transit movement, road traffic management, port and terminal operations, aviation support and pipeline control. Record the conditions that require stopping: unexpected alarms, impaired communications, controller health changes, operator concern or any departure from the approved method. Do not invent a universal packet rate or tolerance.

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

Record the stop and recovery

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

Sources: F01, F03, F06.

Inventory and process dependencies

Build an inventory that explains how assets support rail and transit movement, road traffic management, port and terminal operations, aviation support and pipeline control. 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 unsafe movement, loss of dispatch or signaling visibility, terminal interruption, loss of emergency ventilation, flight-support disruption or pipeline release. Ask engineering to validate the consequence and available protection or manual alternatives.

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

Resolve discrepancies

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

Acceptance

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

Sources: F01, R01, R02.

Network paths and remote access

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

Examine the intended boundary

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

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

Examine the actual access process

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

Prove only what the method establishes

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

Required records

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

Sources: F01, F08.

Accounts legacy systems and suppliers

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

Accounts and authorization

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

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

Support and vulnerability decisions

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

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

Supplier obligations

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

Sources: F01, F08.

Monitoring time and evidence handling

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

Collect a usable record

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

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

Evidence integrity

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

Sensitive information

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

Acceptance

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

Sources: F01, F03, F04.

Recovery and continuity evidence

Check whether the operator can restore the process after loss of rail signaling interfaces, traction-power SCADA, tunnel systems, traffic controllers, terminal cranes, access systems, airport operational support, pipeline SCADA and remote control sites. Backup-job success alone does not establish recovery capability.

Define the restoration objective

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

Examine recovery dependencies

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

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

Exercise and validate

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

Closure evidence

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

Sources: F01, F04, R03.

Authorization for active validation

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

Write an activity permit

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

Choose the least disruptive evidence

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

Confirm readiness at the point of work

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

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

Close the permit

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

Sources: F01, F03, R03.

Writing findings that can be audited

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

Minimum finding record

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

Use precise status

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

Prioritize consequence and uncertainty

Evaluate potential effects on rail and transit movement, road traffic management, port and terminal operations, aviation support and pipeline control, exposure paths, existing safeguards, recovery limits and confidence in the evidence. Include unsafe movement, loss of dispatch or signaling visibility, terminal interruption, loss of emergency ventilation, flight-support disruption or pipeline release where the process supports that consequence. Have engineering review the pathway before presenting it as a fact.

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

Resolve challenge

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

Sources: F01, R01, R02.

Corrective work and management reporting

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

Plan the work

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

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

Report to leadership

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

Report to technical owners

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

Regulatory conclusion

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

Sources: F01, F03.

Verification closure and recurring work

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

Verification procedure

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

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

Handover

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

Recurring triggers

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

Final acceptance

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

Sources: F01, F03, F04.

Facility and applicability worksheet

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

Facility legal entity address and operating function

Ownership operator classification permits registration and contracts

Applicable instruments exact versions and source record IDs

Applicability decisions exceptions and unresolved questions

Operating technical compliance and project owners with alternates

Decision approvers dates next review and authority record

Field activity authorization worksheet

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

Activity purpose exact targets and asset owners

Method tool version permitted functions and excluded actions

Vendor constraints approved traffic behavior and operating baseline

Operating window communications and named stop authority

Recovery support safe response and resumption authority

Operating approval technical approval date and change record

Evidence and finding worksheet

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

Evidence ID source custodian period collection method and integrity

Observed condition and method used to establish it

Applicable requirement exact version and agreed assessment criterion

Operating consequence safeguards assumptions and evidence limits

Finding ID responsible owner priority rationale and challenge

Reviewer disposition date and linked technical record

Corrective action and acceptance worksheet

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

Finding ID action owner dependencies and target date

Approved implementation change record and operating window

Verification criterion authorized method result and evidence IDs

Remaining limitations interim controls and residual risk decision

Operating acceptance compliance disposition and recurring review

Technical reviewer sponsor decision date and closure record

Terms used in the planning records

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

Sources and instrument status

F01 Guide to Operational Technology Security Revision 3

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

F02 Guide to Operational Technology Security Revision 4

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

R01 A survey of cyber security management in industrial control systems

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

R02 Threat modeling of industrial control systems A systematic literature review

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

R03 ICSSIM A framework for building industrial control systems security testbeds

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

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

Sources and instrument status

F03 Technical Guide to Information Security Testing and Assessment

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

F05 CIRCIA public rulemaking notice

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

F09 Cybersecurity Resource Center

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

T01 Cybersecurity in the Marine Transportation System

US Coast Guard and Federal Register. Final rule. 90 FR 6298; 33 CFR 101 Subpart F; 101.605 and 101.630 through 101.665. Check subsequent amendments and operator-specific approval, waivers and equivalents.

T03 Pipeline Cybersecurity Mitigation Actions Contingency Planning and Testing

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

Sources: F03, F05, F09, T01, T03.

Sources and instrument status

T04 Rail Cybersecurity Mitigation Actions and Testing

TSA. Expired directive copy. Security Directive 1580/82-2022-01D; expires May 2 2026. No replacement or extension was authenticated here. Do not issue a current compliance opinion from this expired copy.

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.

T06 Cybersecurity Resources for Transit Agencies

FTA. Agency implementation guidance. 49 USC 5323 v and security directives; distinction between covered operators.

T07 FY2026 Certifications and Assurances

FTA. Agency funding instrument. Current grant certifications and assurances.

T08 Public Transportation Agency Safety Plans

FTA. Agency implementation guidance. 49 CFR Part 673; applicability and safety management. Does not by itself establish the same cyber audit frequency for every transit mode.

Sources: T04, T05, T06, T07, T08.

Sources and instrument status

T09 TSA cybersecurity resource route and unresolved aviation instruments

TSA. Agency routing source; operative instrument unresolved. Obtain the current operator-issued aviation security program and amendments through authorized channels. The former 2023 Year in Review PDF URL returned 404. This agency route is not a replacement operative directive or evidence of current duties.

T02 Maritime cybersecurity implementation timeline

US Coast Guard. Agency implementation notice. January 12 2026 training and July 16 2027 principal compliance milestone. Official indexed notice checked against T01; full-page retrieval restricted.

T10 Maritime cybersecurity current codified provisions

Office of the Federal Register eCFR. Current codified rule. 33 CFR 101.630(f); 101.635; 101.640; 101.650(d)-(e); implementation under 101.655. Current display checked October 13 2026; retrieved provisions reviewed October 16 2026.. Read the applicable compliance dates in 101.655 and any approved equivalent or waiver. The eCFR is authoritative but unofficial.

F07 Emergency Release Notifications under EPCRA

EPA. Agency guidance. EPCRA 304 and CERCLA release notification. Chemical thresholds, release facts and recipients require a separate EHS determination.

F04 Incident Response Recommendations and Considerations Revision 3

NIST. Final guidance. April 2025 final publication.

Sources: T09, T02, T10, F07, F04.

Sources and instrument status

F06 State Plans

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

F08 ISA IEC 62443 Series of Standards

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

Sources: F06, F08.