GLOBAL DIGITAL FORENSICS

OT ASSESSMENT PLANNING PACK

Transportation OT Assessment Planning Pack

Transportation operational technology, industrial control systems and SCADA

Edition 2026-11-03 | November 3, 2026

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

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

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

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

Contents

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

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

What this pack covers

This pack plans an OT security assessment of maritime, rail and transit, pipeline, aviation, port and roadway operations across the United States. Use it with the project workbook and the state and local research companion.

What the assessment produces

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

How current the guidance is

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

Standards behind the method

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

Sign off

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

Sources: F01, F03, F08

Using this planning pack

Use this pack to organize an assessment of 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 starting source register. Those rows are research prompts, not completed facility determinations.

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

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

Reading the evidence

The pack separates binding law or an incorporated instrument, agency guidance, standards, and proposed assessment procedures. A citation identifies the source for a regulatory statement. Procedure descriptions explain how the assessment team collects evidence; obligations come from the governing instruments.

A rule can be effective while a particular requirement has a later compliance date. An approved standard can still be subject to future enforcement. Record both dates and the applicable version. Take deadlines from effective and compliance dates.

Signing an assessment conclusion

The reviewer needs the actual facility facts, current instruments, examined evidence, test permissions and unresolved limitations. A designated technical reviewer reviews the completed work, and the organization then adopts or publishes its conclusions.

Sources: F01, F03

Decisions before mobilization

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 outstanding evidence. State how each exclusion limits the conclusion. An excluded critical dependency must remain visible to the sponsor rather than disappearing from the asset count.

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

Release decision

The sponsor approves purpose and resources. The operating owner approves the process boundary. The compliance owner signs the applicability register. The technical lead signs the method. The project manager records the dependencies and unresolved items. Approval is express.

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. Test movement authority, signaling, runway lighting, emergency ventilation, cranes or pipeline commands in live service only with 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. The operating owner sets the target list and authorizes active tests.
Project manager	Sequences work, tracks evidence and approvals, protects operating windows, manages changes and closes acceptance records.
Evidence custodian and quality reviewer	Control evidence access, integrity, retention and independent review of facts and conclusions. Record conflicts and review exceptions.

Sources: F01, F03

Project stages and acceptance

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

Stage	Required exit evidence
1 Applicability and scope	Signed facility register, controlling instruments, exclusions and reporting scope. Open legal questions have an owner and defined effect on the engagement.
2 Readiness	Approved evidence request, interviews, collection method, secure workspace, current backup evidence and operating contacts.

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

Stage	Required exit evidence
3 Examination	Asset and process records, reconciled diagrams, sampled control evidence and a dated account of what was examined.
4 Authorized validation	Activity permits, baseline observations, test log, stop/recovery record and postwork operating acceptance. Record the validation scope that was authorized.
5 Reporting and decisions	Reviewed findings, requirement mappings, limitations, corrective owners, funding decisions and a residual risk record.
6 Verification and handover	Retest evidence, recurring review schedule, retained records, lessons and signed handover. Recommendations close when verified or formally dispositioned.

Sources: F03

Applicability and obligation records

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

Make a defensible decision

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

Mark an item Not applicable on a documented basis. Lack of a public directive, missing permit or restricted document creates an information gap. Determine whether that gap prevents a compliance conclusion, a test activity, or only a future work item.

Separate obligation types

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

Use the 50 state companion to select additional checks. Confirm municipality, county, tribal or territorial authority where relevant. Municipal ownership can change utility jurisdiction and public entity duties. Independently applicable federal obligations continue.

Preserve the reasoning

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

Sources: F01, F05, F09

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

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. Traffic controller cyber duties come from state, local and contract instruments.
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. Build the clause level assessment basis from the full instrument text.
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

TSA security directives in force

TSA renewed its pipeline and rail directives in May 2026. Audit against the issued directive and the operator’s approved plans.

Pipelines

Security Directive Pipeline-2021-02G, effective May 3, 2026 through May 2, 2027, carries the mitigation, contingency planning and testing duties for notified hazardous liquid and natural gas pipeline and LNG owners and operators. It cancels and supersedes Pipeline-2021-02F. The reporting directive Pipeline-2021-01G, posted January 15, 2026, carries the incident reporting and cybersecurity coordinator duties. Use the operator’s TSA approved Cybersecurity Implementation Plan and Cybersecurity Assessment Plan as the audit basis.

Rail and passenger rail

Security Directive 1580/82-2022-01E, effective May 3, 2026 through May 2, 2027, carries the mitigation and testing duties for freight railroads identified in 49 CFR 1580.101 and other TSA designated freight and passenger railroads. It supersedes 01D. The reporting directives SD 1580-21-01E (rail) and SD 1582-21-01E (public

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

transportation and passenger rail), posted January 15, 2026, carry the incident reporting duties. Obtain the operator's approved Cybersecurity Implementation Plan through the designated security coordinator and protect Sensitive Security Information where it applies.

Aviation

Airport and aircraft operator cybersecurity duties sit in TSA approved security programs and their amendments, which TSA issues to the operator. Request the current program and amendments from the operator security coordinator before scoping aviation work.

Sources: T03, T04, T11, T12, 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. Assign it to every waterfront facility only after 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. Cover the required operational scope directly.

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.

Meet a penetration testing obligation with production safe methods. 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

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

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). Take the initial submission trigger from the instrument. 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

Security Directive 1580/82-2022-01E, effective May 3, 2026 through May 2, 2027, carries the mitigation and testing duties for freight railroads identified in 49 CFR 1580.101 and other TSA designated freight and passenger railroads. It supersedes 01D. The reporting directives SD 1580-21-01E (rail) and SD 1582-21-01E (public transportation and passenger rail), posted January 15, 2026, carry the incident reporting duties. Obtain the operator’s approved Cybersecurity Implementation Plan through the designated security coordinator and protect Sensitive Security Information where it applies.

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.

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

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. Test records are where we look for evidence 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. Traffic injection and failover tests on live signaling run under a signaling specific 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

Security Directive Pipeline-2021-02G, effective May 3, 2026 through May 2, 2027, carries the mitigation, contingency planning and testing duties for notified hazardous liquid and natural gas pipeline and LNG owners and operators. It cancels and supersedes Pipeline-2021-02F. The reporting directive Pipeline-2021-01G, posted January 15, 2026, carries the incident reporting and cybersecurity coordinator duties. Use the operator’s TSA approved Cybersecurity Implementation Plan and Cybersecurity Assessment Plan as the audit basis.

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. Demonstrate a cyber finding with operating settings left as set.

Overlap and reports

Record federal pipeline safety, TSA, state pipeline, environmental and contractual notification criteria separately. Capture the actual event facts and awareness timestamps. File release and safety reports on their own track, and put safe plant response ahead of evidence collection.

Sources: F01, T03, T05, F07

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

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. Aircraft product conformity follows the FAA certification process.

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. Set traffic controller audit intervals from the owning agency's program.

Acceptance

Each responsible operator signs the boundary and permitted method. Each vessel, aircraft, rail signaling system and tenant asset takes its owner's authorization. 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.

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

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, missing 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 tests the plan; restore tests are where we look for evidence of recovery.

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

Interviews that test the record

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

Sampling

Define the control population and sampling rationale. Include material differences in site function, equipment family, criticality, remote access and support arrangements. Draw samples across remote sites so the result describes the whole population. State the sample and the unexamined population in the report.

Readiness evidence

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

Sources: F01, F03

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

Safe work and stop authority

The dispatcher, control room supervisor, port or terminal authority, airport operations lead or pipeline controller retains operating authority. Test movement authority, signaling, runway lighting, emergency ventilation, cranes or pipeline commands in live service only with the appropriate approved operating procedure.

Connecting equipment safely

Attend the operator safety briefing and follow site access, electrical, hazardous energy, confined space and other relevant controls. The operator determines which safety program applies. Electrical switching, confined space entry and plant permits stay with personnel qualified and authorized for them.

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. Set packet rates and tolerances from device specifications.

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

Record the stop and recovery

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

Sources: F01, F03, F06

Inventory and process dependencies

Build an inventory that explains how assets support 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.

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

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. Confirm safety function independence from actual connections.

Resolve discrepancies

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

Acceptance

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

Sources: F01, R01, R02

Network paths and remote access

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

Examine the intended boundary

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

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

Examine the actual access process

Observe a supervised approved support workflow or review retained session records. Record authentication, authorization, account ownership, session visibility, shared account constraints and timeout or revocation behavior. Where an old controller lacks the desired mechanism, evaluate controls at an approved access gateway.

Report what the method tested

Configuration review identifies allowed policy paths; approved validation tests live reachability or exploitation. A controlled connectivity check is a separate authorized activity. A proposed segmentation improvement remains a recommendation until implemented and verified.

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

Required records

Retain the approved path register, source versions, access samples, exceptions and the method used. If ISA/IEC 62443 is contractual, obtain the licensed edition and agreed assessment criteria before claiming conformity. The publicly described zone and conduit approach is a design method.

Sources: F01, F08

Accounts legacy systems and suppliers

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

Accounts and authorization

Review named users, service accounts, vendor accounts and emergency credentials through approved records. Verify owners, privileges, approval, periodic review and revocation evidence. Review how privileged access is separated from normal user activity. Store secrets by reference in the evidence register.

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

Support and vulnerability decisions

Match versions and support status to vendor advisories and approved evidence. Separate a version match, a suspected vulnerability, and a validated condition. Confirm a scanner finding against the installed controller.

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

Supplier obligations

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

Sources: F01, F08

Monitoring time and evidence handling

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

Collect a usable record

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

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

Record timezone, clock source, observed offset and known gaps. If clocks disagree, preserve the original timestamps and the translation used in analysis. A missing event may reflect a collection gap; check logging coverage.

Evidence integrity

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

Sensitive information

Have the compliance owner classify customer information, engineering records and any SSI, CEII, CUI or protected public records. Use the handling rules that actually apply. Privilege and disclosure exemptions rest on their legal tests.

Acceptance

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

Sources: F01, F03, F04

Recovery and continuity evidence

Check whether the operator can restore the process after loss of rail signaling interfaces, traction power SCADA, tunnel systems, traffic controllers, terminal cranes, access systems, airport operational support, pipeline SCADA and remote control sites. Restore tests are where we look for evidence of recovery capability.

Define the restoration objective

Ask operations to identify the minimum service, safe process condition, restoration sequence and maximum tolerable interruption. Record the chosen recovery objectives, their owner and the evidence supporting feasibility. Set recovery targets from the operating requirement.

Examine recovery dependencies

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

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

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

Exercise and validate

Use a scenario with loss of a material dependency. Record which recovery steps were discussed, demonstrated in a representative environment or performed in production under approval. Document differences between the test environment and the installed system. A tabletop exercise tests decisions; restore tests are where we look for evidence of recovery.

Closure evidence

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

Sources: F01, F04, R03

Authorization for active validation

Active validation is optional until a controlling requirement or agreed scope requires it and an acceptable method is authorized. Meet every contractual requirement with a safe operating method.

Write an activity permit

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

Choose the least disruptive evidence

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

Confirm readiness at the point of work

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

Run denial of service, fuzzing, credential guessing, exploit execution, firmware change, controller write or failover only under explicit approval for that method. A necessary activity needs an explicit method, suitable environment and separate approval.

Close the permit

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

Sources: F01, F03, R03

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

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 otherwise. Record a recommendation, implementation and verification as separate states. A screenshot of a configuration change may support implementation without proving that the intended boundary works.

Prioritize consequence and uncertainty

Evaluate potential effects on 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 describes a software vulnerability; consequence analysis is where we assess the plant impact. Record the organization's risk method and acceptance authority. Keep plant risk ratings as precise as the evidence behind them.

Resolve challenge

Give the operating owner a chance to identify incorrect asset facts, missing safeguards and unsafe remediation proposals. Retain the challenge, additional evidence, reviewer decision and revised wording. A disagreement closes with a recorded resolution.

Sources: F01, R01, R02

Corrective work and management reporting

The assessment ends with decisions that an owner can implement and a reviewer can verify. A corrective plan sequences vulnerabilities into operating steps.

Plan the work

For each accepted finding, identify the owner, dependency, required design or procurement, change approval, maintenance window, recovery support, target date and verification evidence. Identify an interim control while the final fix is scheduled. Mark an action Implemented once the work is done.

Sequence actions by operating consequence and dependency. An access boundary may need a maintained jump host, named accounts and supplier support before a legacy controller can be isolated. Verify that the proposed change preserves emergency operation and recovery.

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

Report to leadership

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

Report to technical owners

Provide enough evidence and context to reproduce the observation using the approved method. Identify configuration versions, affected boundary, exceptions and exact acceptance criteria. Include only data the task requires, through approved channels.

Regulatory conclusion

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

Sources: F01, F03

Verification closure and recurring work

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

Verification procedure

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

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

Handover

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

Recurring triggers

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

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

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 that the authorizing official grants.

Activity purpose exact targets and asset owners

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

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

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

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.

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

Term	Meaning in this pack
SSI CEII and CUI	Sensitive Security Information; Critical Energy/Electric Infrastructure Information under the applicable authority; Controlled Unclassified Information. Determine the actual handling regime.
CySO CISO and EHS	Cybersecurity Officer; Chief Information Security Officer; environment health and safety.
PHA MOC and CMMC	Process hazard analysis; management of change; Cybersecurity Maturity Model Certification.
Applicable and Unresolved	Applicable requires facility facts and a controlling instrument. Unresolved identifies a missing fact or authority; Not applicable records a supported basis.

Sources

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

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

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

R01 A survey of cyber security management in industrial control systems. Knowles and colleagues in International Journal of Critical Infrastructure Protection. Peer reviewed research. Volume 9 June 2015 pages 52 to 80. Used for qualitative management context, not contemporary law or numeric effectiveness claims. https://doi.org/10.1016/j.ijcip.2015.02.002 (checked October 15, 2026)

R02 Threat modeling of industrial control systems A systematic literature review. Computers and Security. Peer reviewed research. Volume 136 January 2024 article 103543. Supports structured threat modeling for use in a specific plant assessment. https://doi.org/10.1016/j.cose.2023.103543 (checked October 15, 2026)

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

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

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

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

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

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. https://www.federalregister.gov/documents/2025/01/17/2025-00708/cybersecurity-in-the-marine-transportation-system (checked October 15, 2026)

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

T04 Rail Cybersecurity Mitigation Actions and Testing. TSA. Current security directive. Security Directive 1580/82-2022-01E, effective May 3, 2026 through May 2, 2027; supersedes 1580/82-2022-01D; freight railroads in 49 CFR 1580.101 and other TSA designated freight and passenger railroads. https://www.tsa.gov/sites/default/files/signed_security_directive_1580_82-2022-01e_and_transmittal_memo_508c.pdf (checked November 3, 2026)

T05 Pipeline control room management. PHMSA. Agency implementation guidance. 49 CFR 192.631 and 195.446; controller and SCADA scope. These are safety requirements alongside any applicable TSA cybersecurity instrument. https://www.phmsa.dot.gov/pipeline/control-room-management/control-room-management (checked October 15, 2026)

T06 Cybersecurity Resources for Transit Agencies. FTA. Agency implementation guidance. 49 USC 5323 v and security directives; distinction between covered operators. https://www.transit.dot.gov/regulations-and-programs/safety/cybersecurity-resources-transit-agencies (checked October 15, 2026)

T07 FY2026 Certifications and Assurances. FTA. Agency funding instrument. Current grant certifications and assurances. https://www.transit.dot.gov/funding/grants/grantee-resources/certifications-and-assurances/fy2026-annual-list-certifications (checked October 15, 2026)

T08 Public Transportation Agency Safety Plans. FTA. Agency implementation guidance. 49 CFR Part 673; applicability and safety management. Cyber audit frequency is set mode by mode for transit. https://www.transit.dot.gov/PTASP (checked October 15, 2026)

T09 TSA security directives and emergency amendments. TSA. Agency index. Aviation security programs and amendments are issued to the operator; request the current program from the airport or aircraft operator security coordinator. https://www.tsa.gov/sd-and-ea (checked November 3, 2026)

T11 Enhancing Pipeline Cybersecurity, Security Directive Pipeline-2021-01G. TSA. Current security directive. Posted January 15, 2026; incident reporting and cybersecurity coordinator directive for notified pipeline owners and operators. https://www.tsa.gov/sd-and-ea (checked November 3, 2026)

T12 Enhancing Rail Cybersecurity, SD 1580-21-01E, and Enhancing Public Transportation and Passenger Railroad Cybersecurity, SD 1582-21-01E. TSA. Current security directives. Posted January 15, 2026; incident reporting and coordinator directives for rail and passenger rail. https://www.tsa.gov/sd-and-ea (checked November 3, 2026)

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

T02 Maritime cybersecurity implementation timeline. US Coast Guard. Agency implementation notice. January 12 2026 training and July 16 2027 principal compliance milestone. Official notice checked against T01. https://www.news.uscg.mil/maritime-commons/Article/4247529/final-rule-cybersecurity-in-the-marine-transportation-system-implementation-tim/ (checked October 15, 2026)

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. https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F (checked October 15, 2026)

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. https://www.epa.gov/epcra/epcra-emergency-release-notifications (checked October 15, 2026)

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

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

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

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

Plan the assessment with a senior examiner

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

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

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

Request a consultation online at evestigate.com/contact.

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