GLOBAL DIGITAL FORENSICS

OT ASSESSMENT PLANNING PACK

Manufacturing OT Assessment Planning Pack

Manufacturing 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. Manufacturing regulatory scope
8. Process safety and change management
9. Defense information and contract boundaries
10. Production cell and quality examination
11. Manufacturing incident and restart exercise
12. Manufacturing recurring calendar
13. Document requests and interviews
14. Safe work and stop authority
15. Inventory and process dependencies
16. Network paths and remote access
17. Accounts legacy systems and suppliers
18. Monitoring time and evidence handling
19. Recovery and continuity evidence
20. Authorization for active validation
21. Writing findings that can be audited
22. Corrective work and management reporting
23. Verification closure and recurring work
24. Facility and applicability worksheet
25. Field activity authorization worksheet
26. Evidence and finding worksheet
27. Corrective action and acceptance worksheet
28. Terms used in the planning records
29. Sources

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

What this pack covers

This pack plans an OT security assessment of production cells, process control, safety systems, quality records and plant networks 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 production cells, batch processing, robotics, process control, safety functions, utilities and product release. 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

Identify each legal entity, site and production process. Screen chemical process safety, environmental permits, defense information, federal contracts and regulated product requirements separately. Sector instruments set federal OT assessment mandates.

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 PLCs, DCS and SIS interfaces, robots, CNC machines, HMIs, engineering tools, MES links, historians, quality systems and remote maintenance connections. 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. Production and safety personnel control machine operation, safeguarding and hazardous energy. Keep interlocks and guarding in service, recipes and controller logic unchanged, and safety systems connected only to approved equipment.
Compliance owner and counsel	Resolve applicable instruments, disclosure restrictions and incident reporting duties. Identify the responsible filing official and alternate.
Technical lead and field technician	Design the permitted method and collect traceable evidence. The operating owner sets the target list and authorizes active tests.
Project manager	Sequences work, tracks evidence and approvals, protects operating windows, manages changes and closes acceptance records.
Evidence custodian and quality reviewer	Control evidence access, integrity, retention and independent review of facts and conclusions. Record conflicts and review exceptions.

Sources: F01, F03

Project stages and acceptance

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

Stage	Required exit evidence
1 Applicability and scope	Signed facility register, controlling instruments, exclusions and reporting scope. Open legal questions have an owner and defined effect on the engagement.
2 Readiness	Approved evidence request, interviews, collection method, secure workspace, current backup evidence and operating contacts.
3 Examination	Asset and process records, reconciled diagrams, sampled control evidence and a dated account of what was examined.

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

Stage	Required exit evidence
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.

Manufacturing regulatory scope

There is no single federal SCADA cybersecurity audit rule that can be assigned to every US manufacturer from its sector label. Determine the applicable process, product and contractual regimes.

Chemical process and environmental scope

Screen the actual process and substance inventories for OSHA PSM and EPA Risk Management Program coverage. Coordinate cyber findings that affect process hazards, safeguards or operating procedures with the responsible process safety and EHS owners. A cyber review complements the PHA, mechanical integrity program and permit assessment.

Defense and federal contracts

Determine whether a contract contains DFARS 252.204-7012 or another safeguarding and reporting clause. Identify covered defense information, the system that processes it and any designated operationally critical support. Define the CUI boundary system by system, including each PLC.

Product and quality systems

For regulated products, identify predicate records, quality system requirements, validated processes and the quality unit. FDA Part 11 scope depends on the applicable records and predicate requirements. Apply it to the historians and HMIs within its scope. Product specific validation duties require their own qualified review.

State and local overlay

Review state plan safety jurisdiction, environmental permits, public entity or government contractor status, data breach duties and local chemical/emergency arrangements. An insurer's cybersecurity statute applies to its defined licensees.

Sources: F06, F07, M01, M02, M05, M09

Process safety and change management

Where PSM applies, coordinate the cybersecurity work with the existing process safety program and the qualified people responsible for it.

Map a cyber condition to the process

Identify the process hazard, affected control or safeguard, credible initiating path and available independent protections. Engineering and process safety confirm the assumptions. A potential recipe or setpoint change be presented as a demonstrated physical outcome only with suitable evidence.

Examine existing management records

Review process safety information, relevant PHA findings, operating procedures, maintenance records, management of change decisions and training. For a proposed network or controller change, ask whether it affects a covered process or a credited safeguard. Route the decision through the established change process.

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

Keep audit types distinct

OSHA 1910.119(o) requires evaluation of PSM compliance at least every three years for covered processes. That three year cycle belongs to its own program. A cyber control assessment supplies evidence to a PSM review, which the full PSM audit then incorporates.

Work authorization

Follow site hazardous energy, electrical, machine safeguarding and other work controls. Cyber assessors verify findings with safety instrumented functions in service and plant permits followed. Use controlled records and suitable representative systems when live work is unacceptable.

Sources: F01, F06, M01, M05

Defense information and contract boundaries

Use the awarded contract and current written direction. Regulatory history gives useful context; the instrument governing the engagement controls.

Establish the information boundary

Identify the contract, clause version, required CMMC status if any, covered information, approved system boundary and relevant subcontract flowdowns. Trace whether engineering drawings, recipes, production instructions or maintenance records actually contain covered information. Record the determination and responsible contracting and information owners.

Current implementation status

A July 13 2026 official agency announcement reports suspension of the planned CMMC Phase II rollout originally scheduled for November 10 2026. Confirm the full text and current procurement direction with the contracting officer. Read the historical phase date as history, and keep existing contract clauses in force until the contract is modified.

Obtain current agency direction and contracting officer interpretation, then record the requirement governing the specific award. Keep applicable safeguarding duties under DFARS 252.204-7012 and any other contract obligations in force unless a valid controlling instrument changes them.

Incident and evidence duties

Where DFARS 252.204-7012 applies, the clause requires rapid covered cyberincident reporting within 72 hours of discovery and preservation of images and relevant monitoring or packet data for at least 90 days from report submission. Validate the trigger, current clause and reporting route. Send CUI and detailed incident evidence through approved channels.

Sources: M02, M03, M04

Production cell and quality examination

Use the production flow to select evidence. Include how a change can affect people, product and the ability to restart.

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

Control and engineering path

Identify PLC, DCS, robot and CNC engineering access, project files, approved logic versions, recipes and change approvals. Examine how the production team confirms the correct version and who can authorize a download. Review supplier access and support dependencies.

Safety and product consequences

Separate normal control from safety related functions. Trace whether a cyber condition could alter a safeguard, measurement, batch record, product specification or release decision. Ask the responsible safety or quality owner to verify the pathway and existing checks.

Production and enterprise interfaces

Review MES, ERP, historian, laboratory and quality links relevant to the scoped process. Identify whether a corporate outage blocks production, traceability, shipping or recovery. Determine the permitted local or degraded mode, who authorizes it and how records are reconciled afterwards.

Recovery evidence

Verify the availability of trusted controller projects, machine parameters, robot programs, supplier licenses, firmware and spares. Review representative restoration evidence. After a server is restored, confirm the cell is safe, product data is correct and the quality unit has approved restart.

Sources: F01, M01, M07, M09, R03

Manufacturing incident and restart exercise

The following scenario is fictional. The exercise tests decisions, approvals and evidence rather than manipulating a production recipe.

Scenario

A support workstation is suspected of compromise while the line is producing a regulated or safety critical product. A recipe record differs from the approved copy. Next, establish the controller state and the affected production interval.

Test the response

Production and safety determine the safe operating response. Quality decides product hold and release criteria where applicable. The technical team preserves relevant evidence using an approved method. Engineering identifies the authoritative recipe and logic records and the limits of a comparison.

Test obligation decisions

The compliance owner evaluates contract cyber reporting, environmental or safety consequences, personal data incidents and customer notification clauses. The quality unit decides product release, and the plant's reporting officials decide chemical reporting thresholds.

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

Test restart acceptance

Locate the approved recovery materials and change process. Define who must accept machine operation, safeguards, product genealogy and record integrity before restart. Record remaining uncertainty and a named corrective owner. No exercise outcome should be described as an actual production validation.

Sources: F04, M01, M02, M09

Manufacturing recurring calendar

Build the schedule around the actual process, contracts and change program.

Program	Scheduling decision
OT assessment and supplier access	Use the adopted risk program and contract. Contracts, permits and sector rules set manufacturer assessment cycles. Review material production and access changes.
PSM where covered	Map PHA, management of change, training, mechanical integrity and at least three year compliance audit duties to the responsible process safety program.
Defense contract where covered	Record the exact safeguarding, assessment, affirmation, reporting and evidence retention obligations in the current contract. Resolve CMMC implementation uncertainty before setting a phase deadline.
Product and environmental regime	Identify the quality unit, validated systems, predicate records, permits, EHS reporting and local emergency arrangements. Obtain specialist review for product specific duties.
CFATS and changing instruments	The reviewed CISA notice reports expiry of statutory authorization in 2023. Confirm reauthorization status from current law. Keep as an unresolved legislative check rather than an assumed active 2026 obligation.

Sources: M01, M02, M03, M04, M05, M06, M09

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 PLCs, DCS and SIS interfaces, robots, CNC machines, HMIs, engineering tools, MES links, historians, quality systems and remote maintenance connections. 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.

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

Interviews that test the record

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

Sampling

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

Readiness evidence

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

Sources: F01, F03

Safe work and stop authority

Production and safety personnel control machine operation, safeguarding and hazardous energy. Keep interlocks and guarding in service, recipes and controller logic unchanged, and safety systems connected only to approved equipment.

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 production cells, batch processing, robotics, process control, safety functions, utilities and product release. 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.

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

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 production cells, batch processing, robotics, process control, safety functions, utilities and product release. 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 injury, hazardous release, defective product, lost traceability, scrapped work in progress or prolonged loss of production. 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.

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

Examine the intended boundary

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

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

Examine the actual access process

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

Report what the method tested

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

Required records

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

Sources: F01, F08

Accounts legacy systems and suppliers

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

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.

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

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

Supplier obligations

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

Sources: F01, F08

Monitoring time and evidence handling

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

Collect a usable record

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

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

Evidence integrity

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

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

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

Recovery and continuity evidence

Check whether the operator can restore the process after loss of PLCs, DCS and SIS interfaces, robots, CNC machines, HMIs, engineering tools, MES links, historians, quality systems and remote maintenance connections. Restore tests are where we look for evidence of recovery capability.

Define the restoration objective

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

Examine recovery dependencies

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

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

Exercise and validate

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

Closure evidence

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

Sources: F01, F04, R03

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.

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

Choose the least disruptive evidence

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

Confirm readiness at the point of work

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

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

Close the permit

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

Sources: F01, F03, R03

Writing findings that can be audited

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

Minimum finding record

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

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 production cells, batch processing, robotics, process control, safety functions, utilities and product release, exposure paths, existing safeguards, recovery limits and confidence in the evidence. Include injury, hazardous release, defective product, lost traceability, scrapped work in progress or prolonged loss of production 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.

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

Resolve challenge

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

Sources: F01, R01, R02

Corrective work and management reporting

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

Plan the work

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

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

Report to leadership

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

Report to technical owners

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

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.

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

Verification procedure

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

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

Handover

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

Recurring triggers

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

Final acceptance

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

Sources: F01, F03, F04

Facility and applicability worksheet

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

Facility legal entity address and operating function

Ownership operator classification permits registration and contracts

Applicable instruments exact versions and source record IDs

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

Applicability decisions exceptions and unresolved questions
Operating technical compliance and project owners with alternates
Decision approvers dates next review and authority record

Field activity authorization worksheet

The operating owner approves the activity before work. This worksheet records permission that the authorizing official grants.

Activity purpose exact targets and asset owners
Method tool version permitted functions and excluded actions
Vendor constraints approved traffic behavior and operating baseline
Operating window communications and named stop authority
Recovery support safe response and resumption authority
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.

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

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

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

Technical reviewer sponsor decision date and closure record

Terms used in the planning records

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

Sources

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

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)

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

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)

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)

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)

M01 Process safety management of highly hazardous chemicals. OSHA. Federal regulation. Paragraphs e j l m and o; PHA, mechanical integrity, management of change and compliance audits. Coverage is process and substance dependent. The three year PSM audit covers process safety management. https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.119 (checked October 15, 2026)

M02 Safeguarding Covered Defense Information and Cyber Incident Reporting. Acquisition gov. Federal contract clause. DFARS 252.204-7012; covered information and rapid reporting. The contract, incorporated revision and system boundary control applicability. https://www.acquisition.gov/dfars/part-252-solicitation-provisions-and-contract-clauses#DFARS_252.204-7012 (checked November 3, 2026)

M05 Risk Management Program guidance. EPA. Agency guidance. 40 CFR Part 68 applicability and program levels. Cybersecurity certification comes from a cyber specific instrument. https://www.epa.gov/rmp/general-rmp-guidance-introduction (checked October 15, 2026)

M09 Electronic Records and Electronic Signatures Scope and Application. FDA. Agency guidance. 21 CFR Part 11 and predicate rule records. Determine the actual regulated records and product regime; not every PLC record is automatically within Part 11. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application (checked October 15, 2026)

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

M03 CMMC Phase II suspension announcement. Office of Industrial Base Growth. Official agency announcement. July 13, 2026 Phase II suspension, carried in Class Deviation 2026-O0025 Rev 3. Official content reports suspension of the planned Phase II rollout. Confirm current procurement direction with the contracting officer; existing contracts change through formal modification. https://business.defense.gov/Engage/News/Article/4542563/forging-the-arsenal-of-freedom-department-of-war-suspends-cmmc-phase-ii-require/ (checked October 15, 2026)

M04 CMMC program documentation. Defense CIO. Program source. Program instruments and contract implementation. Reconcile current instructions with M03 and the awarded contract before using historical phase dates. https://dodcio.defense.gov/CMMC/Documentation/ (checked October 15, 2026)

M07 Manufacturing Profile Revision 1. NIST. Final guidance. October 2020 final profile aligned to CSF 1.1. https://csrc.nist.gov/pubs/ir/8183/r1/final (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)

M06 CFATS program status. CISA. Archived agency notice. Statutory authorization expired July 28 2023. Confirm reauthorization status from current law. Read an archived CFATS checklist as program history. https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats (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.