

Manufacturing OT assessment planning pack

Planning edition October 16, 2026

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

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

Purpose

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

Working records

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

Facility adoption

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

Contents

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

3 Planning scope and research basis	20 Accounts legacy systems and suppliers
4 Using the corrected workbook edition	21 Monitoring time and evidence handling
5 Using this planning pack	22 Recovery and continuity evidence
6 Decisions before mobilization	23 Authorization for active validation
7 Roles and decision authority	24 Writing findings that can be audited
8 Project stages and acceptance	25 Corrective work and management reporting
9 Applicability and obligation records	26 Verification closure and recurring work
10 Manufacturing regulatory scope	27 Facility and applicability worksheet
11 Process safety and change management	28 Field activity authorization worksheet
12 Defense information and contract boundaries	29 Evidence and finding worksheet
13 Production cell and quality examination	30 Corrective action and acceptance worksheet
14 Manufacturing incident and restart exercise	31 Terms used in the planning records
15 Manufacturing recurring calendar	32 Sources and instrument status
16 Document requests and interviews	33 Sources and instrument status
17 Safe work and stop authority	34 Sources and instrument status
18 Inventory and process dependencies	35 Sources and instrument status
19 Network paths and remote access	

Planning scope and research basis

This pack supports a controlled assessment of production cells, batch processing, robotics, process control, safety functions, utilities and product release in the United States. Use the companion volume to screen all 50 states and resolve the actual local and facility requirements.

What the assessment produces

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

Research cutoff

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

Open applicability

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

Adoption and review

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

Sources: [F01](#), [F02](#), [R01](#), [R02](#), [R03](#).

Using the corrected workbook edition

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

Before execution

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

Open and incomplete decisions

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

Scope and authority

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

Source access and revision

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

Sources: [F01](#), [F03](#).

Using this planning pack

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

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

Reading the evidence

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

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

Before signing an assessment conclusion

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

Sources: [F01](#), [F03](#).

Decisions before mobilization

Identify each legal entity, site and production process. Screen chemical-process safety, environmental permits, defense information, federal contracts and regulated product requirements separately. NAICS classification alone does not establish a federal OT assessment mandate.

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

Release decision

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

Sources: [F01](#), [F03](#).

Roles and decision authority

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

Role	Decision or work owned
Sponsor or CISO	Approves business objective, resources and reporting audience. Accepts residual business risk only within delegated authority.
Operating owner and engineering authority	Approve process boundaries, safe state and production methods. Production and safety personnel control machine operation, safeguarding and hazardous energy. Do not bypass interlocks, defeat guarding, alter a recipe, download controller logic or connect unapproved equipment to a safety system.
Compliance owner and counsel	Resolve applicable instruments, disclosure restrictions and incident-reporting duties. Identify the responsible filing official and alternate.
Technical lead and field technician	Design the permitted method and collect traceable evidence. A technician cannot expand the target list or authorize an active test.
Project manager	Sequences work, tracks evidence and approvals, protects operating windows, manages changes and closes acceptance records.
Evidence custodian and quality reviewer	Control evidence access, integrity, retention and independent review of facts and conclusions. Record conflicts and review exceptions.

Sources: [F01](#), [F03](#).

Project stages and acceptance

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

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

Sources: F03.

Applicability and obligation records

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

Make a defensible decision

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

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

Separate obligation types

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

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

Preserve the reasoning

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

Sources: [F01](#), [F05](#), [F09](#).

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 does not replace a PHA, mechanical-integrity program or 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. A factory serving a defense customer does not automatically put every PLC inside one CUI boundary.

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. It is not a blanket labeling rule for every historian or HMI. 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 and must not be borrowed as a manufacturing rule.

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 must not be presented as a demonstrated physical outcome without 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.

Keep audit types distinct

OSHA 1910.119(o) requires evaluation of PSM compliance at least every three years for covered processes. That is not a general three-year OT cybersecurity assessment mandate. A cyber control assessment can supply evidence to a PSM review but does not by itself satisfy the full PSM audit.

Work authorization

Follow site hazardous-energy, electrical, machine-safeguarding and other work controls. Cyber assessors cannot bypass a safety instrumented function, enter a hazardous area or exercise equipment simply to verify a finding. 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 is useful context but cannot substitute for the instrument governing the engagement.

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 uncertainty

A July 13 2026 official agency announcement reports suspension of the planned CMMC Phase II rollout originally scheduled for November 10 2026. Full text and the complete current procurement direction were not authenticated here. Do not use the historical phase date as a current universal deadline, or infer that the announcement removes an existing contract clause.

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 cyber-incident 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. Do not send CUI or detailed incident evidence through unapproved 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.

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. A restored server does not establish that the cell is safe, product data is correct or 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. The controller state and affected production interval are not yet established.

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. An assessor does not decide that a product is safe for release or that a chemical reporting threshold was not crossed.

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. No uniform statutory annual cycle for all manufacturers was established. 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. No current reauthorization was established. 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. Allow a supervised review when a copy cannot leave the site. Record evidence not supplied and the effect of that limitation. Never request credentials or live network diagrams through a public inquiry form.

Interviews that test the record

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

Sampling

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

Readiness evidence

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

Sources: [F01](#), [F03](#).

Safe work and stop authority

Production and safety personnel control machine operation, safeguarding and hazardous energy. Do not bypass interlocks, defeat guarding, alter a recipe, download controller logic or connect unapproved equipment to a safety system.

Before connecting anything

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

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

Define measurable stop conditions

Operations defines the baseline process indicators and limits appropriate to 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. Do not invent a universal packet rate or tolerance.

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

Record the stop and recovery

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

Sources: [F01](#), [F03](#), [F06](#).

Inventory and process dependencies

Build an inventory that explains how assets support 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. Do not assume a safety function remains independent because it appears in a different diagram layer.

Resolve discrepancies

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

Acceptance

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

Sources: [F01](#), [R01](#), [R02](#).

Network paths and remote access

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

Examine the intended boundary

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

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

Examine the actual access process

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

Prove only what the method establishes

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

Required records

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

Sources: [F01](#), [F08](#).

Accounts legacy systems and suppliers

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

Accounts and authorization

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

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

Support and vulnerability decisions

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

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

Supplier obligations

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

Sources: [F01](#), [F08](#).

Monitoring time and evidence handling

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

Collect a usable record

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

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

Evidence integrity

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

Sensitive information

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

Acceptance

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

Sources: [F01](#), [F03](#), [F04](#).

Recovery and continuity evidence

Check whether the operator can restore the process after loss of PLCs, DCS and SIS interfaces, robots, CNC machines, HMIs, engineering tools, MES links, historians, quality systems and remote maintenance connections. Backup-job success alone does not establish recovery capability.

Define the restoration objective

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

Examine recovery dependencies

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

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

Exercise and validate

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

Closure evidence

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

Sources: [F01](#), [F04](#), [R03](#).

Authorization for active validation

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

Write an activity permit

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

Choose the least disruptive evidence

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

Confirm readiness at the point of work

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

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

Close the permit

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

Sources: [F01](#), [F03](#), [R03](#).

Writing findings that can be audited

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

Minimum finding record

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

Use precise status

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

Prioritize consequence and uncertainty

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

Resolve challenge

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

Sources: [F01](#), [R01](#), [R02](#).

Corrective work and management reporting

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

Plan the work

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

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

Report to leadership

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

Report to technical owners

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

Regulatory conclusion

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

Sources: [F01](#), [F03](#).

Verification closure and recurring work

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

Verification procedure

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

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

Handover

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

Recurring triggers

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

Final acceptance

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

Sources: [F01](#), [F03](#), [F04](#).

Facility and applicability worksheet

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

Facility legal entity address and operating function

Ownership operator classification permits registration and contracts

Applicable instruments exact versions and source record IDs

Applicability decisions exceptions and unresolved questions

Operating technical compliance and project owners with alternates

Decision approvers dates next review and authority record

Field activity authorization worksheet

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

Activity purpose exact targets and asset owners

Method tool version permitted functions and excluded actions

Vendor constraints approved traffic behavior and operating baseline

Operating window communications and named stop authority

Recovery support safe response and resumption authority

Operating approval technical approval date and change record

Evidence and finding worksheet

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

Evidence ID source custodian period collection method and integrity

Observed condition and method used to establish it

Applicable requirement exact version and agreed assessment criterion

Operating consequence safeguards assumptions and evidence limits

Finding ID responsible owner priority rationale and challenge

Reviewer disposition date and linked technical record

Corrective action and acceptance worksheet

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

Finding ID action owner dependencies and target date

Approved implementation change record and operating window

Verification criterion authorized method result and evidence IDs

Remaining limitations interim controls and residual risk decision

Operating acceptance compliance disposition and recurring review

Technical reviewer sponsor decision date and closure record

Terms used in the planning records

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

Sources and instrument status

F01 Guide to Operational Technology Security Revision 3

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

F02 Guide to Operational Technology Security Revision 4

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

R01 A survey of cyber security management in industrial control systems

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

R02 Threat modeling of industrial control systems A systematic literature review

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

R03 ICSSIM A framework for building industrial control systems security testbeds

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

Sources: [F01](#), [F02](#), [R01](#), [R02](#), [R03](#).

Sources and instrument status

F03 Technical Guide to Information Security Testing and Assessment

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

F05 CIRCIA public rulemaking notice

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

F09 Cybersecurity Resource Center

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

F06 State Plans

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

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.

Sources: [F03](#), [F05](#), [F09](#), [F06](#), [F07](#).

Sources and instrument status

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 is not a universal OT cybersecurity audit rule.

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.

M05 Risk Management Program guidance

EPA. Agency guidance. 40 CFR Part 68 applicability and program levels. Covered chemical process duties do not create a generic cybersecurity certification.

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.

M03 CMMC Phase II suspension announcement

Office of Industrial Base Growth. Official agency announcement. July 13 2026 announcement. Official indexed content reports suspension of the planned Phase II rollout. Full-page retrieval was restricted. Obtain current procurement direction and contracting-officer interpretation; do not infer amendment of an existing contract.

Sources: [M01](#), [M02](#), [M05](#), [M09](#), [M03](#).

Sources and instrument status

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.

M07 Manufacturing Profile Revision 1

NIST. Final guidance. October 2020 final profile aligned to CSF 1.1.

F04 Incident Response Recommendations and Considerations Revision 3

NIST. Final guidance. April 2025 final publication.

M06 CFATS program status

CISA. Archived agency notice. Statutory authorization expired July 28 2023. No current reauthorization was established here. Do not treat an archived CFATS checklist as proof of an active 2026 duty.

F08 ISA IEC 62443 Series of Standards

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

Sources: [M04](#), [M07](#), [F04](#), [M06](#), [F08](#).