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

MANUFACTURING OT ASSESSMENT PLANNING MANUAL

The Manufacturing OT Assessment Manual for Assessing Without Stopping the Line

A production line keeps its schedule, and every scan in a plant assessment is planned to fit around it. This manual from Global Digital Forensics gives plant managers, controls engineers and compliance owners a complete planning record for an assessment that respects that schedule.

Planning scope and research basis

This manual is built for a controlled assessment of production cells, batch processing, robotics, process control, safety functions, utilities and product release at facilities in the United States. It carries the federal and sector research; the companion volume screens all fifty states so you can resolve the local permits, state plan jurisdiction and facility requirements that apply at the state and local level.

What the assessment produces

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

Sources current to November 3, 2026

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

Open applicability

The source register gives binding instruments, guidance, drafts, superseded versions and open questions their own entries.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

Adoption and review

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

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

If an open applicability item is holding up a decision you have to make now, call (800) 868-8189 and a senior practitioner will help you identify the controlling text to obtain.

Sources: F01 Guide to Operational Technology Security Revision 3, F02 Guide to Operational Technology Security Revision 4, R01 A survey of cyber security management in industrial control systems, R02 Threat modeling of industrial control systems A systematic literature review, R03 ICSSIM A framework for building industrial control systems security testbeds

---

Applying the Updated Audit Workbook

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

Pre Execution Readiness Checklist

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

Pending Scope and Governance Decisions

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

Engagement Scope and Authorization

Record every proposed exclusion, its reason and the responsible reviewer in Scope decisions so deferred work stays visible to the sponsor. The State research sheet is a separately labelled routing register: its state and sector rows are a client research checklist, and a row becomes part of a facility conclusion once the controlling instrument is retrieved and recorded beside it. For New York work use the Clause matrix and questions Q01 to Q10 in the New York set. A current instrument or local fact that is being gathered stays marked Unresolved, and the mark changes when someone retrieves the text or establishes the fact.

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

Source Access and Revision History

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

Sources: F01 Guide to Operational Technology Security Revision 3, F03 Technical Guide to Information Security Testing and Assessment

---

Using this planning pack

Work through this pack in the order a plant actually makes decisions. Fix the legal and operating boundary first, because the contract, the permit and the process hazard analysis decide what an assessment of production cells, robotics, process control and product release is allowed to touch. Choose evidence and methods once the people who own the process have agreed what may be examined, so the assessment serves production and runs alongside it.

First use

Read the sector applicability pages, then the State and local applicability companion. Create one record for each legal entity, facility and regulatory program. The workbook's state and sector rows form a client research checklist, with a separate register of fifty state starting sources; a row becomes a facility determination when the operator records the instrument and the decision, and that record is what lets the plant defend the finding. Appoint a sponsor, an operating owner, a technical lead, a compliance owner and a project manager. Complete the site worksheet. Resolve the mandatory instruments and the operating permissions before scheduling any intrusive work, and use the field authorization sheet for each approved activity.

Reading the evidence

The pack separates binding law or an incorporated instrument, agency guidance, standards and proposed assessment procedures. A citation identifies the source for a regulatory statement. A procedure description explains how the assessment team can collect evidence, and the legal obligations themselves come from the cited instruments. A rule can be effective while a particular requirement carries a later compliance date, and an approved standard can be subject to future enforcement. Record both dates and the applicable version, and take each deadline from the instrument's effective date.

Before signing an assessment conclusion

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

Work the pack with the people named under First use, and when the boundary is fixed, request a free assessment scope built around it.

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

Sources: F01 Guide to Operational Technology Security Revision 3, F03 Technical Guide to Information Security Testing and Assessment

Decisions before mobilization

Identify each legal entity, site and production process before anyone opens a checklist. Screen chemical process safety, environmental permits, defense information, federal contracts and regulated product requirements as separate questions, because each one attaches to a different part of the plant and answers to a different owner. A NAICS code describes what the plant makes, and a federal OT assessment duty comes from a specific instrument, which is the first thing an auditor will ask to see.

Define the work product

Decide in writing whether the engagement is an engineering risk assessment, a gap assessment against named requirements, independent assurance, or a combination with the responsibilities separated. The decision changes the evidence standard, the sampling and the words the report may use. Name the intended recipients and who may receive the technical appendices. If the assessment team or its firm designed, installed or operates any of the controls in scope, disclose that relationship before any part of the work is described as independent.

Record the facility boundary

Identify PLCs, DCS and SIS interfaces, robots, CNC machines, HMIs, engineering tools, MES links, historians, quality systems and remote maintenance connections. Include the identity, DNS, time, virtualization, telecommunications and backup dependencies whose failure could affect the process, because the services that can actually take the process down belong in the record alongside the controller. Identify shared corporate services and third party interfaces explicitly, and record that naming them in the boundary leaves test permission with the activity permits. For each legal entity record the physical address, owner, operator, sector, production or service function, permits, regulators, contracts, insurer conditions and public body status. For distributed assets list every other state, local authority and control center involved.

Define exclusions

Document every excluded safety system, vendor appliance held outside the access arrangements, firmware past vendor support, protocol held back from testing and record awaiting production, and state in one sentence how each exclusion shapes the conclusion. An excluded critical dependency stays in the report as a visible scope decision that the sponsor accepted. Holding the asset count steady from scoping to report keeps the scope matched to the estate rather than to what was convenient to examine.

Release decision

The sponsor approves purpose and resources. The operating owner approves the process boundary. The compliance owner signs the applicability register. The technical lead signs the method. The project manager records the dependencies and the open items. Each signature is dated and kept with the scope record, and

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

approval is that written signature, given by each of these people in turn.

Sources: F01 Guide to Operational Technology Security Revision 3, F03 Technical Guide to Information Security Testing and Assessment

Roles and decision authority

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

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

Sources: F01 Guide to Operational Technology Security Revision 3, F03 Technical Guide to Information Security Testing and Assessment

Project stages and acceptance

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

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

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

Sources: F03 Technical Guide to Information Security Testing and Assessment

---

Applicability and obligation records

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

Make a defensible decision

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

Separate obligation types

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

Preserve the reasoning

The compliance owner signs the decision date and the next review trigger. Save the instrument and its source URL in controlled records and name the person who will watch for amendments. For an incident clock record the trigger event, the start timestamp with its time zone, the deadline rule, the recipient, the permitted channel,

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

the responsible official and the receipt. The auditor's first question about any applicability decision is why it was made and by whom, and this record is the only acceptable answer.

Sources: F01 Guide to Operational Technology Security Revision 3, F05 CIRCIA public rulemaking notice, F09 Cybersecurity Resource Center

---

Manufacturing regulatory scope

Federal SCADA cybersecurity audit duties reach a United States manufacturer through specific instruments tied to its process, product and contracts, rather than through a single rule attached to its sector label. The regimes that reach the plant floor arrive through the process chemistry, the product, the customer contract and the state, and the first job is to determine which of them actually apply to the installed systems.

Chemical process and environmental scope

Screen the actual process and the substance inventories for OSHA PSM and EPA Risk Management Program coverage, using the covered chemical list and the threshold quantities rather than a general impression that the plant handles chemicals. Where coverage exists, coordinate every cyber finding that affects process hazards, safeguards or operating procedures with the responsible process safety and EHS owners, and route the finding through their records.

Defense and federal contracts

Determine whether a contract contains DFARS 252.204-7012 or another safeguarding and reporting clause, and obtain the clause text from the awarded contract rather than from a summary. Identify the covered defense information, the system that processes it and any designated operationally critical support. For a factory serving a defense customer, the CUI boundary follows the information flow PLC by PLC, and it is drawn from the data flow record and the contract rather than from the customer's logo on the shipping label.

Product and quality systems

For regulated products identify the predicate records, the quality system requirements, the validated processes and the quality unit. FDA Part 11 scope depends on the applicable records and the predicate requirements, so each historian and HMI is assessed on the records it actually holds. Product specific validation duties require their own qualified review, and the assessment's job is to show which control system records feed a regulated decision and who owns their integrity.

State and local overlay

Review state plan safety jurisdiction, environmental permits, public entity or government contractor status, data breach duties and the local chemical and emergency arrangements.

Sources: F06 State Plans, F07 Emergency Release Notifications under EPCRA, M01 Process safety management of highly hazardous chemicals, M02 Safeguarding Covered Defense Information and Cyber Incident Reporting, M05 Risk Management Program guidance, M09 Electronic Records and Electronic

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

Signatures Scope and Application

Process safety and change management

Where PSM applies, the cybersecurity work runs inside the existing process safety program and under the qualified people responsible for it. The assessment borrows their records, their hazard analysis and their change process, and works inside that one program.

Map a cyber condition to the process

Identify the process hazard, the affected control or safeguard, the credible initiating path and the available independent protections. Engineering and process safety confirm the assumptions, and their confirmation is recorded with a name and a date. A potential recipe or setpoint change is reported as a hypothesis, and it moves to a demonstrated event when suitable evidence of the physical outcome has been examined.

Examine existing management records

Review the process safety information, the relevant PHA findings, the operating procedures, the maintenance records, the management of change decisions and the training records. For every proposed network or controller change ask whether it affects a covered process or a credited safeguard, and route the decision through the established change process. The management of change file is the artifact an auditor will open first, because it shows whether the plant actually controls what reaches the controller.

Keep audit types distinct

OSHA 1910.119(o) requires an evaluation of PSM compliance at least every three years for covered processes. That is a process safety audit cycle, and OT cybersecurity assessment timing comes from the program or contract that covers the plant. A cyber control assessment can supply evidence to a PSM review, the PSM compliance audit is a separate evaluation, and the two reports are written and filed as separate records.

Work authorization

Follow the site's hazardous energy, electrical, machine safeguarding and other work controls exactly as a contractor would. Cyber assessors verify findings through controlled records, observation and suitable representative systems, while safety instrumented functions, hazardous areas and equipment operation stay with the plant's qualified personnel. Where live work is set aside, the finding names the method used in its place.

Sources: F01 Guide to Operational Technology Security Revision 3, F06 State Plans, M01 Process safety management of highly hazardous chemicals, M05 Risk Management Program guidance

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

Defense information and contract boundaries

Use the awarded contract and the current written direction from the contracting officer. Regulatory history is useful context, the governing instrument sets the requirement, and the assessment record names which instrument that is.

Establish the information boundary

Identify the contract, the clause version, the required CMMC status if any, the covered information, the approved system boundary and the relevant subcontract flowdowns. Trace whether engineering drawings, recipes, production instructions or maintenance records actually contain covered information by following the data from receipt to the controller and the historian. Record the determination together with the responsible contracting and information owners, because the boundary decision is theirs to sign.

Current implementation status

On July 13, 2026 the Department of War Chief Information Officer suspended the CMMC Phase 2 transition planned for November 10, 2026, and Class Deviation 2026-O0025 Revision 3 carries that direction into solicitations and contracts. Obtain the current agency direction and the contracting officer's interpretation, then record the requirement that governs the specific award. Safeguarding duties under DFARS 252.204-7012 and any other contract obligations stay in force, and a change to them comes through a valid controlling instrument.

Incident and evidence duties

Where DFARS 252.204-7012 applies, the clause requires rapid reporting of a covered cyber incident 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, the current clause and the reporting route before an incident, and rehearse them in the exercise.

Sources: M02 Safeguarding Covered Defense Information and Cyber Incident Reporting, M03 CMMC Phase II suspension announcement, M04 CMMC program documentation

Production cell and quality examination

Use the production flow to select evidence, starting from the product that leaves the dock and working back to the controllers that made it. Include at each step how a change could affect people, product and the ability to restart.

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

Control and engineering path

Identify the PLC, DCS, robot and CNC engineering access, the project files, the approved logic versions, the recipes and the change approvals. Request the controller project files with their stored checksums and a compare report against the running logic, because the comparison between the approved version and the running version is the single most informative artifact in a plant assessment. Examine how the production team confirms the correct version and who can authorize a download. Review supplier access and support dependencies on the same path.

Safety and product consequences

Separate normal control from safety related functions. Trace whether a cyber condition could alter a safeguard, a measurement, a batch record, a product specification or a release decision, and ask the responsible safety or quality owner to verify the pathway and the existing checks. The report records their verification as the basis for the finding.

Production and enterprise interfaces

Review the MES, ERP, historian, laboratory and quality links relevant to the scoped process. Identify whether a corporate outage blocks production, traceability, shipping or recovery, and determine the permitted local or degraded mode, who authorizes it and how records are reconciled afterwards. The exercise is where a plant names the person authorized to declare degraded mode, and many plants make that appointment there for the first time.

Recovery evidence

Verify the availability of trusted controller projects, machine parameters, robot programs, supplier licenses, firmware and spares. Review representative restoration evidence, and record the cell safety, product data and quality restart acceptances, each with its own owner.

Sources: F01 Guide to Operational Technology Security Revision 3, M01 Process safety management of highly hazardous chemicals, M07 Manufacturing Profile Revision 1, M09 Electronic Records and Electronic Signatures Scope and Application, R03 ICSSIM A framework for building industrial control systems security testbeds

---

Manufacturing incident and restart exercise

The following scenario is fictional. The exercise tests decisions, approvals and evidence while the production recipe stays untouched, and its value lies in settling who decides what.

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. Establishing the controller state and the affected production interval is the next task.

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

Test the response

Production and safety determine the safe operating response. Quality decides the product hold and release criteria where applicable. The technical team preserves the relevant evidence using an approved method and records the hash and the time of each capture. Engineering identifies the authoritative recipe and logic records and explains how a comparison between them and the running controller is read and corroborated.

Test obligation decisions

The compliance owner evaluates contract cyber reporting, environmental or safety consequences, personal data incidents and customer notification clauses, each on its own clock. Product release and chemical reporting threshold decisions belong to the quality and EHS owners, and the exercise record names who made each one.

Test restart acceptance

Locate the approved recovery materials and the change process. Define who must accept machine operation, safeguards, product genealogy and record integrity before restart, and have each of them say so in the exercise. Record the open questions and a named corrective owner. Exercise outcomes are described as exercise results, and production validation is recorded as its own separately approved activity.

Sources: F04 Incident Response Recommendations and Considerations Revision 3, M01 Process safety management of highly hazardous chemicals, M02 Safeguarding Covered Defense Information and Cyber Incident Reporting, M09 Electronic Records and Electronic Signatures Scope and Application

---

Manufacturing recurring calendar

Build the schedule around the actual process, the contracts and the change program rather than around a generic annual cycle. Each row names the record that proves the duty was met.

Program	Scheduling decision
OT assessment and supplier access	Use the adopted risk program and the contract. The assessment cycle comes from the contract, program or rule that covers the plant, and it varies from one manufacturer to the next. Review after material production changes and after any change to supplier remote access.
PSM where covered	Map the PHA, management of change, training, mechanical integrity and at least three year compliance audit duties to the responsible process safety program and its records.
Defense contract where covered	Record the exact safeguarding, assessment, affirmation, reporting and evidence retention obligations in the current contract. Confirm the current CMMC implementation direction, then set any phase deadline.

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

Program	Scheduling decision
Product and environmental regime	Identify the quality unit, the validated systems, the predicate records, the permits, the EHS reporting and the 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, and the research record carries reauthorization as an open legislative check. Confirm the current status with CISA before recording any CFATS duty as active for 2026.

Sources: M01 Process safety management of highly hazardous chemicals, M02 Safeguarding Covered Defense Information and Cyber Incident Reporting, M03 CMMC Phase II suspension announcement, M04 CMMC program documentation, M05 Risk Management Program guidance, M06 CFATS program status, M09 Electronic Records and Electronic Signatures Scope and Application

Document requests and interviews

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

Initial evidence request

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

Interviews that test the record

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

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

Sampling

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

Readiness evidence

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

Sources: F01 Guide to Operational Technology Security Revision 3, F03 Technical Guide to Information Security Testing and Assessment

---

Safe work and stop authority

Production and safety personnel control machine operation, safeguarding and hazardous energy. These sentences are the operating rule for the entire engagement, and every member of the assessment team can repeat them from memory before the first site day.

Before connecting anything

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

Define measurable stop conditions

Operations defines the baseline process indicators and limits appropriate to production cells, batch processing, robotics, process control, safety functions, utilities and product release. Record the conditions that require stopping in the operator's own terms: unexpected alarms, impaired communications, controller health changes, operator concern or any departure from the approved method. The number that matters is the one the operator watches. Name who can stop work and who can authorize resumption. Any technician may call a safety stop. The operating owner directs the plant response, including any isolation, device reset or process restart, and the assessor follows that direction.

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

Record the stop and recovery

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

Sources: F01 Guide to Operational Technology Security Revision 3, F03 Technical Guide to Information Security Testing and Assessment, F06 State Plans

---

Inventory and process dependencies

Build an inventory that explains how each asset supports production cells, batch processing, robotics, process control, safety functions, utilities and product release. A working inventory reconciles IP address lists and passive discovery exports against the drawings and ties each entry to the process it supports.

Use existing evidence first

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

Trace the consequence

For each critical process trace the route from the operator interface and the control logic through communications to field equipment and the supporting services. Identify how an asset failure could contribute to injury, hazardous release, defective product, lost traceability, scrapped work in progress or prolonged loss of production. Ask engineering to validate the consequence and the available protection or manual alternative, then write down what they said and who said it. Record protective functions separately from normal process control and document the dependencies on identity, time sources, licensing, cloud support, third party communications and engineering tools. A safety function counts as independent when engineering has shown you how it is isolated, whatever layer of the drawing it appears in.

Resolve discrepancies

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

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

Deliverable Review and Acceptance Criteria

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

Sources: F01 Guide to Operational Technology Security Revision 3, R01 A survey of cyber security management in industrial control systems, R02 Threat modeling of industrial control systems A systematic literature review

---

Network paths and remote access

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

Examine the intended boundary

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

Examine the actual access process

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

Match each claim to its method

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

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

Required records

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

Sources: F01 Guide to Operational Technology Security Revision 3, F08 ISA/IEC 62443 Series of Standards

---

Accounts, legacy systems and suppliers

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

Accounts and authorization

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

Support and vulnerability decisions

Match versions and support status to vendor advisories using approved evidence. Separate a version match, a suspected vulnerability and a validated condition, and keep them separate in the finding register. A controller that answers a scan slowly is a reason to stop and review the scan plan. For a legacy device compare patch availability, vendor support, maintenance dependencies, network exposure, replacement lead time and restoration options. The assessment recommends a decision. Operations and engineering approve changes under their own change process.

Supplier obligations

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

Sources: F01 Guide to Operational Technology Security Revision 3, F08 ISA/IEC 62443 Series of Standards

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

Monitoring, time and evidence handling

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

Collect a usable record

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

Evidence integrity

Assign each item a stable evidence identifier and record its origin, custodian, collection date and method, source period, filename or record reference, integrity value where appropriate, storage location and access history. Keep originals protected and conduct analysis on controlled working copies. Log every transformation and redaction. This is the discipline that lets a finding survive challenge from a vendor, a regulator or opposing counsel, and it costs minutes at collection time against hours of argument later.

Sensitive information

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

Deliverable Review and Acceptance Criteria

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

Sources: F01 Guide to Operational Technology Security Revision 3, F03 Technical Guide to Information Security Testing and Assessment, F04 Incident Response Recommendations and Considerations Revision 3

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

Define the restoration objective

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

Examine recovery dependencies

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

Exercise and validate

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

Closure evidence

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

Sources: F01 Guide to Operational Technology Security Revision 3, F04 Incident Response Recommendations and Considerations Revision 3, R03 ICSSIM A framework for building industrial control systems security testbeds

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

Authorization for active validation

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

Write an activity permit

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

Choose the least disruptive evidence

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

Confirm readiness at the point of work

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

Close the permit

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

Sources: F01 Guide to Operational Technology Security Revision 3, F03 Technical Guide to Information Security Testing and Assessment, R03 ICSSIM A framework for building industrial control systems security testbeds

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

Writing findings that can be audited

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

Minimum finding record

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

Use precise status

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

Prioritize consequence and uncertainty

Evaluate the potential effects on production cells, batch processing, robotics, process control, safety functions, utilities and product release, the exposure paths, the existing safeguards, the recovery limits and the 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, and have engineering review the pathway before it is presented as fact. A CVSS score describes a software vulnerability, and plant risk comes from the organization's own method. Record that risk method and the acceptance authority, and build the plant risk rating from it so its precision matches the evidence.

Resolve challenge

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

Sources: F01 Guide to Operational Technology Security Revision 3, R01 A survey of cyber security management in industrial control systems, R02 Threat modeling of industrial control systems A systematic literature review

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

Corrective work and management reporting

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

Plan the work

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

Report to leadership

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

Report to technical owners

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

Regulatory conclusion

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

Sources: F01 Guide to Operational Technology Security Revision 3, F03 Technical Guide to Information Security Testing and Assessment

Verification closure and recurring work

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

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

Verification procedure

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

Evidence Handover and Chain of Custody Transfer

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

Recurring triggers

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

Final acceptance

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

Sources: F01 Guide to Operational Technology Security Revision 3, F03 Technical Guide to Information Security Testing and Assessment, F04 Incident Response Recommendations and Considerations Revision 3

Facility and applicability worksheet

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

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

Evidentiary Record Fields

Facility legal entity address and operating function

Ownership operator classification permits registration and contracts

Applicable instruments exact versions and source record IDs

Applicability decisions exceptions and unresolved questions

Operating technical compliance and project owners with alternates

Decision approvers dates next review and authority record

Field activity authorization worksheet

The operating owner approves the activity before work begins. This worksheet records that permission.

Evidentiary Record Fields

Activity purpose exact targets and asset owners

Method tool version permitted functions and excluded actions

Vendor constraints approved traffic behavior and operating baseline

Operating window communications and named stop authority

Recovery support safe response and resumption authority

Operating approval technical approval date and change record

Evidence and finding worksheet

Record facts separately from possible consequences. Link the original evidence, preserve the source times and state the method and its scope, so any qualified reviewer can reproduce the finding from the record.

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

Evidentiary Record Fields

Evidence ID source custodian period collection method and integrity

Observed condition and method used to establish it

Applicable requirement exact version and agreed assessment criterion

Operating consequence safeguards assumptions and evidence limits

Finding ID responsible owner priority rationale and challenge

Reviewer disposition date and linked technical record

Corrective action and acceptance worksheet

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

Evidentiary Record Fields

Finding ID action owner dependencies and target date

Approved implementation change record and operating window

Verification criterion authorized method result and evidence IDs

Remaining limitations interim controls and residual risk decision

Operating acceptance compliance disposition and recurring review

Technical reviewer sponsor decision date and closure record

Terms used in the planning records

Term	Meaning in this pack
OT ICS and SCADA	Operational technology; industrial control systems; supervisory control and data acquisition.
PLC RTU HMI DCS SIS	Programmable logic controller; remote terminal unit; human machine interface; distributed control system; safety instrumented system.

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

Term	Meaning in this pack
RRA ERP and PWSID	Risk and resilience assessment; emergency response plan; public water system identifier.
BES CIP DER and EMS DMS	Bulk Electric System; Critical Infrastructure Protection; distributed energy resources; energy/distribution management system.
SSI CEII and CUI	Sensitive Security Information; Critical Energy/Electric Infrastructure Information under the applicable authority; Controlled Unclassified Information. Determine the actual handling regime.
CySO CISO and EHS	Cybersecurity Officer; Chief Information Security Officer; environment health and safety.
PHA MOC and CMMC	Process hazard analysis; management of change; Cybersecurity Maturity Model Certification.
Applicable and Unresolved	Applicable requires facility facts and a controlling instrument. Unresolved marks a fact or authority awaiting confirmation, and it is a separate status from Not applicable.

Sources F01 to R03, federal guidance and peer reviewed research

F01 Guide to Operational Technology Security Revision 3

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

F02 Guide to Operational Technology Security Revision 4

NIST. Draft guidance. September 21 2026 initial public draft. Revision 4 was released as an initial public draft on September 21, 2026, so Revision 3 remains the final baseline.

R01 A survey of cyber security management in industrial control systems

Knowles and colleagues in International Journal of Critical Infrastructure Protection. Peer reviewed research. Volume 9 June 2015 pages 52 to 80. Used for qualitative management context, while current law and any effectiveness figures come from the primary instruments.

R02 Threat modeling of industrial control systems A systematic literature review

Computers and Security. Peer reviewed research. Volume 136 January 2024 article 103543. Supports structured threat modeling, and each plant assessment is validated on its own evidence.

R03 ICSSIM A framework for building industrial control systems security testbeds

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

Sources: F01 Guide to Operational Technology Security Revision 3, F02 Guide to Operational Technology Security Revision 4, R01 A survey of cyber security management in industrial control systems, R02 Threat modeling of industrial control systems A systematic literature review, R03 ICSSIM A framework for building

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

industrial control systems security testbeds

Sources F03 to F07, federal guidance

F03 Technical Guide to Information Security Testing and Assessment

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

F05 CIRCIA public rulemaking notice

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

F09 Cybersecurity Resource Center

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

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 Technical Guide to Information Security Testing and Assessment, F05 CIRCIA public rulemaking notice, F09 Cybersecurity Resource Center, F06 State Plans, F07 Emergency Release Notifications under EPCRA

Sources M01 to M03, manufacturing instruments

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, and the three year PSM audit is a process safety compliance audit, separate from OT cybersecurity assessment.

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

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 are risk management program duties and stand apart from any 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, and test each PLC record against the predicate rules before placing it within Part 11.

M03 CMMC Phase II suspension announcement

Office of Industrial Base Growth. Official agency announcement. July 13 2026 announcement. The Department of War Chief Information Officer memorandum of July 13, 2026 suspends the November 2026 Phase 2 transition. Obtain current procurement direction and contracting officer interpretation.

Sources: M01 Process safety management of highly hazardous chemicals, M02 Safeguarding Covered Defense Information and Cyber Incident Reporting, M05 Risk Management Program guidance, M09 Electronic Records and Electronic Signatures Scope and Application, M03 CMMC Phase II suspension announcement

---

Sources M04 to F08, federal guidance and manufacturing instruments

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. Confirm the program's current status with CISA, then record any CFATS duty accordingly.

F08 ISA/IEC 62443 Series of Standards

ISA. Standards publisher overview. Published series and applicable parts. The normative texts are licensed from ISA and IEC, and a conformity or security level claim rests on the licensed edition the organization holds.

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

Sources: M04 CMMC program documentation, M07 Manufacturing Profile Revision 1, F04 Incident Response Recommendations and Considerations Revision 3, M06 CFATS program status, F08 ISA/IEC 62443 Series of Standards

READY TO PLAN THE ASSESSMENT?

Plan the Manufacturing Assessment With Examiners Who Respect the Line

The manual gives you the records, the roles and the stop authority. Global Digital Forensics supplies the examiners who turn them into a scoped assessment: court tested forensic specialists who have served businesses and their counsel since 1992, who start with passive evidence, authorize every active step by name and write findings an auditor, a customer or a contracting officer can follow. Tell us about the process, the installed systems and the contract requirements in play, and we will scope the work with your production and safety leads. The first consultation is free.

Web Addresses for the Sources Cited

1. F01 Guide to Operational Technology Security Revision 3: https://csrc.nist.gov/pubs/sp/800/82/r3/final
2. F02 Guide to Operational Technology Security Revision 4: https://csrc.nist.gov/pubs/sp/800/82/r4/ipd
3. R01 A survey of cyber security management in industrial control systems: https://doi.org/10.1016/j.ijcip.2015.02.002
4. R02 Threat modeling of industrial control systems A systematic literature review: https://doi.org/10.1016/j.cose.2023.103543
5. R03 ICSSIM A framework for building industrial control systems security testbeds: https://doi.org/10.1016/j.compind.2023.103906
6. F03 Technical Guide to Information Security Testing and Assessment: https://csrc.nist.gov/pubs/sp/800/115/final
7. F05 CIRCIA public rulemaking notice: https://public-inspection.federalregister.gov/2026-10417.pdf
8. F09 Cybersecurity Resource Center: https://www.dfs.ny.gov/industry_guidance/cybersecurity
9. F06 State Plans: https://www.osha.gov/stateplans/
10. F07 Emergency Release Notifications under EPCRA: https://www.epa.gov/epcra/epcra-emergency-release-notifications
11. M01 Process safety management of highly hazardous chemicals: https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.119
12. M02 Safeguarding Covered Defense Information and Cyber Incident Reporting: https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
13. M05 Risk Management Program guidance: https://www.epa.gov/rmp/general-rmp-guidance-introduction
14. M09 Electronic Records and Electronic Signatures Scope and Application: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application
15. M03 CMMC Phase II suspension announcement: https://business.defense.gov/Engage/News/Article/4542563/forging-the-arsenal-of-freedom-department-of-war-suspends-cmmc-phase-ii-require/
16. M04 CMMC program documentation: https://dodcio.defense.gov/CMMC/Documentation/
17. M07 Manufacturing Profile Revision 1: https://csrc.nist.gov/pubs/ir/8183/r1/final
18. F04 Incident Response Recommendations and Considerations Revision 3: https://csrc.nist.gov/pubs/sp/800/61/r3/final
19. M06 CFATS program status: https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats
20. F08 ISA/IEC 62443 Series of Standards: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

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

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

Start With a Free Consultation

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

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

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