GLOBAL DIGITAL FORENSICS

OT ASSESSMENT PLANNING PACK

Water and Wastewater OT Assessment Planning Pack

Water and wastewater operational technology, industrial control systems and SCADA

Edition 2026-11-03 | November 3, 2026

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

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

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

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

Contents

1. What this pack covers
2. Using this planning pack
3. Decisions before mobilization
4. Roles and decision authority
5. Project stages and acceptance
6. Applicability and obligation records
7. Federal drinking water obligations
8. Wastewater and discharge obligations
9. State water requirements that change the plan
10. Water process examination
11. Water incident and continuity exercise
12. Water reporting and recurring calendar
13. Document requests and interviews
14. Safe work and stop authority
15. Inventory and process dependencies
16. Network paths and remote access
17. Accounts legacy systems and suppliers
18. Monitoring time and evidence handling
19. Recovery and continuity evidence
20. Authorization for active validation
21. Writing findings that can be audited
22. Corrective work and management reporting
23. Verification closure and recurring work
24. Facility and applicability worksheet
25. Field activity authorization worksheet
26. Evidence and finding worksheet
27. Corrective action and acceptance worksheet
28. Terms used in the planning records
29. Sources

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

What this pack covers

This pack plans an OT security assessment of treatment, disinfection, pumping, storage, distribution, collection and effluent control across the United States. Use it with the project workbook and the state and local research companion.

What the assessment produces

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

How current the guidance is

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

Standards behind the method

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

Sign off

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

Sources: F01, F03, F08

Using this planning pack

Use this pack to organize an assessment of treatment, disinfection, pumping, storage, distribution, collection and effluent control. Start with the legal and operating boundary. Select evidence and methods only after the people responsible for the process agree what may be examined.

First use

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

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

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

Reading the evidence

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

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

Signing an assessment conclusion

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

Sources: F01, F03

Decisions before mobilization

Distinguish community drinking water systems, noncommunity water systems, publicly owned treatment works, private wastewater facilities and industrial dischargers. Record population, service connections and customers as separate quantities.

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 and RTUs, SCADA servers, HMIs, engineering stations, dosing controllers, telemetry, remote pump stations, laboratory interfaces and vendor connections. Include supporting identity, DNS, time, virtualization, telecommunications and backup dependencies when their failure could affect the process. Identify shared corporate services and third party interfaces without silently expanding test permission.

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

Define exclusions

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

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

Release decision

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

Sources: F01, F03

Roles and decision authority

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

Role	Decision or work owned
Sponsor or CISO	Approves business objective, resources and reporting audience. Accepts residual business risk only within delegated authority.
Operating owner and engineering authority	Approve process boundaries, safe state and production methods. Water operations determine safe treatment, pressure, chemical dosing and discharge conditions. Setpoints, dosing rates, alarm limits and controller modes stay with operators.
Compliance owner and counsel	Resolve applicable instruments, disclosure restrictions and incident reporting duties. Identify the responsible filing official and alternate.
Technical lead and field technician	Design the permitted method and collect traceable evidence. The operating owner sets the target list and authorizes active tests.
Project manager	Sequences work, tracks evidence and approvals, protects operating windows, manages changes and closes acceptance records.
Evidence custodian and quality reviewer	Control evidence access, integrity, retention and independent review of facts and conclusions. Record conflicts and review exceptions.

Sources: F01, F03

Project stages and acceptance

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

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

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

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

Sources: F03

Applicability and obligation records

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

Make a defensible decision

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

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

Separate obligation types

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

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

Preserve the reasoning

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

Sources: F01, F05, F09

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

Federal drinking water obligations

AWIA Section 2013 amended SDWA Section 1433. Its RRA and ERP duties apply to community drinking water systems serving more than 3,300 people. This federal certification duty covers community water systems.

Scope and content

Record each PWSID, community system status and population served. The complete RRA extends beyond cyber risk and includes physical systems, monitoring, financial infrastructure, chemicals and operation and maintenance. Map cyber evidence into the complete RRA rather than presenting a standalone scan as the statutory assessment.

Certification sequence

The second cycle RRA dates were March 31 2025 for systems serving 100,000 or more, December 31 2025 for 50,000 to 99,999, and June 30 2026 for 3,301 to 49,999. Confirm the actual certification receipt. ERP certification is due within six months of actual RRA certification, which can be earlier than a cohort maximum.

EPA lists December 31 2026 as the latest ERP date for the 3,301 to 49,999 cohort when the RRA was certified at its final due date. A missing receipt requires reconciliation now, not assignment of a new six month period from this assessment. Subsequent five year review and certification duties need their own calendar.

Evidence and filing

Retain the completed RRA, ERP, cyber contribution, approved revisions, certification statements and acknowledgments. EPA instructs utilities to submit certifications rather than the actual plans and to keep the plans securely for at least five years. Coordinate with the local emergency planning committee to the extent possible as required by the program.

Sources: W01, W02

Wastewater and discharge obligations

Treat wastewater facilities as their own regulatory population. State law and a facility permit can impose cyber duties independently of AWIA.

Establish the permit boundary

Record the NPDES or state permit, publicly owned treatment works status, outfalls, collection systems, remote pump sites, industrial pretreatment obligations and emergency conditions. Identify which owner or operator is responsible for reporting a malfunction, bypass, release or loss of treatment capability.

Connect cyber events to physical reporting

An unauthorized account event and a sewer overflow can trigger different reporting duties. Evaluate both the cyber event and the process consequence. Obtain the current permit and state instructions for notification timing, channel and follow up. Wait for a full forensic cause determination after escalating a possible time sensitive operational report.

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

New York example

DEC identifies initial reporting by SPDES permittees as soon as possible and no later than 24 hours after awareness, plus a second report within 30 days. Its adopted 2026 rules distinguish those incident duties from POTW emergency planning, training, access, network and vulnerability requirements. The compendium identifies March 11 2027 for specified POTW requirements and March 28 2027 for initial annual certification.

Operational evidence

Trace collection and treatment alarms, telemetry dependencies, pump controls, disinfection and effluent monitoring. Examine how personnel detect loss of visibility, verify actual conditions, contact the permit authority and maintain an approved safe operating response. EPA's wastewater ERP template is useful guidance; SDWA 1433 certification applies to community water systems.

Sources: W03, W10, W11

State water requirements that change the plan

Use the 50 state companion for every facility. The examples below require separate population units and schedules.

State and source	Planning action
Indiana W04	Screen covered computerized/SCADA facilities, including specified community water and wastewater categories. Verify the 500 person water threshold. Separate annual assessment by December 31 from 2026, certification every other year from December 31 2026, and annual August 31 reporter designation.
Maryland W05 W06	Use more than 3,300 customers under Environment 9-2705 for enhanced scope. Confirm the July 1 2026 maturity assessment and two year cycle. Reconcile agency certification collection with actual operator submission instructions.
New Jersey W07 W08	Use more than 500 service connections for WQAA scope (N.J.S.A. 58:31-2). The cybersecurity program must cover every industrial control system and conform to the NIST Cybersecurity Framework, the CIS Controls or ISO/IEC 27000. Join NJCCIC, report each cybersecurity incident to NJCCIC promptly after an employee becomes aware of it, and expect an NJCCIC audit within 30 days of a report (58:31-4.2). Confirm any separate BPU order.
New York W09 W10 W11	Separate DOH drinking water duties from DEC wastewater duties. Appendix 5-E covers community water systems serving more than 3,300 people: operator training and incident reports to DOH within 24 hours have applied since adoption on March 11, 2026, and the 48 hour vulnerability report, the cybersecurity program and the annual vulnerability analysis apply from January 1, 2027. DEC requires every SPDES permittee to report a cybersecurity incident within 24 hours (from March 26, 2026) with a 30 day written report; POTW controls and emergency response plans apply from March 11, 2027, with the first annual certification due March 28, 2027.
Missouri S25 and New Hampshire S29 NH-WW	Evaluate statutory Internet connected control exemptions and other stated exceptions. A disconnected system keeps its safety, incident and permit duties.

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

Sources: W04, W05, W06, W07, W08, W09, W10, W11, S25, S29, NH-WW

Water process examination

Build separate evidence paths for safe treatment, distribution continuity and wastewater consequences.

Treatment and dosing

Identify how approved chemical setpoints, recipes or control logic are established, changed, checked and restored. Examine access approvals and change evidence. Ask operations how an incorrect value would be detected by independent measurement or operator checks. Dosing stays with operators; findings come from records.

Remote pumping and telemetry

Record communications ownership, remote asset access, loss of comms behavior, operator alarms, local operating capability and physical access. Examine one representative current communication loss or recovery record if available. Any live interruption or controller failover requires a separate approved operating test.

Laboratory and reporting interfaces

Trace the data used to make treatment, public health and discharge decisions. Review access, time integrity, retained records and exceptions when data is missing or unreliable. Establish who can validate field measurements and authorize public or regulatory communication.

Evidence accepted

The operator validates the process diagram and the credible consequence scenarios. Link each weakness to the affected service and safeguards. Preserve uncertainty where process interlocks, manual operation or alarm effectiveness were described but not demonstrated.

Sources: F01, W01, W03

Water incident and continuity exercise

Use an exercise to test decisions and records without manipulating a live process. The following scenario is fictional.

Scenario

A vendor account is suspected of unauthorized access to a remote pumping environment. Telemetry values are inconsistent; confirm the actual process condition next. An operator also reports a communications alarm.

Controller prompts

Ask the operating lead to establish the safe response and independent condition checks. Ask the technical team to identify the access path, relevant records and time uncertainty. Ask the compliance owner to determine whether state cyber reporting, a permit report, a public health notification or a contract notice is triggered.

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

Test the decisions

Record the first awareness timestamp, event classifications, alternate communications, available credentials held securely, supplier reachability and authority to change remote access. Test whether the team can locate the current ERP and the actual regulator contacts while normal corporate systems are down.

Acceptance and correction

The observer records decisions, supporting evidence, elapsed times only if measured, missing contacts and unsafe assumptions. Assign an owner to every unresolved issue. A tabletop result records the decision process; restore tests and regulator records are where we look for recovery and acceptance.

Sources: F04, W03, W10

Water reporting and recurring calendar

Populate the calendar from signed applicability decisions and actual prior completion records.

Record	Trigger and evidence
AWIA RRA and ERP	Track each PWSID, population cohort, actual certification dates, ERP dependency and five year review cycle. Retain acknowledgments and current plans.
State program	Record applicable annual or two year assessment, certification, training and framework update duties separately. Keep the state cycle alongside AWIA's five year cycle.
Operational event	Use the current permit and state definition for treatment failure, loss of safe service, bypass, overflow or discharge. Record the separate initial and written follow up clocks.
Cyber incident	For applicable Indiana facilities, IDEM identifies 24 hours after discovery when operations are affected and two business days otherwise. Check current reporting instructions and concurrent public entity duties.
Physical and organizational change	Review whether the change triggers a new analysis, plan revision, regulator notice or recertification. Keep the change decision and the source establishing the trigger.

Sources: W01, W02, W04, W05, W06, W08, W09, W10

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 and RTUs, SCADA servers, HMIs, engineering stations, dosing controllers, telemetry, remote pump stations, laboratory interfaces and vendor connections. Ask for the applicable regulatory assessments, prior findings and change history.

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

Give each request an identifier, purpose, expected owner, time period, format and due date. Offer supervised onsite review when copies stay onsite. Record outstanding evidence and its effect on the conclusion. Exchange credentials and live diagrams through secure channels.

Interviews that test the record

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

Sampling

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

Readiness evidence

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

Sources: F01, F03

Safe work and stop authority

Water operations determine safe treatment, pressure, chemical dosing and discharge conditions. Setpoints, dosing rates, alarm limits and controller modes stay with operators.

Connecting equipment safely

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

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

Define measurable stop conditions

Operations defines the baseline process indicators and limits appropriate to treatment, disinfection, pumping, storage, distribution, collection and effluent control. Record the conditions that require stopping: unexpected alarms, impaired communications, controller health changes, operator concern or any departure from the approved method. Set packet rates and tolerances from device specifications.

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

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

Record the stop and recovery

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

Sources: F01, F03, F06

Inventory and process dependencies

Build an inventory that explains how assets support treatment, disinfection, pumping, storage, distribution, collection and effluent control. A list of IP addresses alone is insufficient.

Use existing evidence first

Reconcile engineering inventories, configuration exports, approved drawings, maintenance records and supervised physical observations. Record asset identifier, function, location, owner, manufacturer, model, firmware/software, support status, protocol, zone and recovery dependency. Distinguish observed values from information supplied by a vendor or operator.

Trace the consequence

For each critical process, trace the route from operator interface and control logic to communications, field equipment and supporting services. Identify how an asset failure could contribute to loss of treatment control, unsafe chemical dosing, loss of distribution pressure, sewer overflow or impaired effluent monitoring. Ask engineering to validate the consequence and available protection or manual alternatives.

Record protective functions separately from normal process control. Document dependencies on identity, time sources, licensing, cloud support, third party communications and engineering tools. Confirm safety function independence from actual connections.

Resolve discrepancies

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

Acceptance

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

Sources: F01, R01, R02

Network paths and remote access

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

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

Examine the intended boundary

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

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

Examine the actual access process

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

Report what the method tested

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

Required records

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

Sources: F01, F08

Accounts legacy systems and suppliers

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

Accounts and authorization

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

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

Support and vulnerability decisions

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

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

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

Supplier obligations

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

Sources: F01, F08

Monitoring time and evidence handling

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

Collect a usable record

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

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

Evidence integrity

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

Sensitive information

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

Acceptance

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

Sources: F01, F03, F04

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

Recovery and continuity evidence

Check whether the operator can restore the process after loss of PLCs and RTUs, SCADA servers, HMIs, engineering stations, dosing controllers, telemetry, remote pump stations, laboratory interfaces and vendor connections. Restore tests are where we look for evidence of recovery capability.

Define the restoration objective

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

Examine recovery dependencies

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

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

Exercise and validate

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

Closure evidence

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

Sources: F01, F04, R03

Authorization for active validation

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

Write an activity permit

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

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

Choose the least disruptive evidence

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

Confirm readiness at the point of work

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

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

Close the permit

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

Sources: F01, F03, R03

Writing findings that can be audited

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

Minimum finding record

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

Use precise status

Use Observed when the available evidence establishes a condition. Use Suspected or Unresolved otherwise. Record a recommendation, implementation and verification as separate states. A screenshot of a configuration change may support implementation without proving that the intended boundary works.

Prioritize consequence and uncertainty

Evaluate potential effects on treatment, disinfection, pumping, storage, distribution, collection and effluent control, exposure paths, existing safeguards, recovery limits and confidence in the evidence. Include loss of treatment control, unsafe chemical dosing, loss of distribution pressure, sewer overflow or impaired effluent monitoring where the process supports that consequence. Have engineering review the pathway before presenting it as a fact.

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

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

Resolve challenge

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

Sources: F01, R01, R02

Corrective work and management reporting

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

Plan the work

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

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

Report to leadership

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

Report to technical owners

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

Regulatory conclusion

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

Sources: F01, F03

Verification closure and recurring work

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

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

Verification procedure

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

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

Handover

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

Recurring triggers

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

Final acceptance

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

Sources: F01, F03, F04

Facility and applicability worksheet

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

Facility legal entity address and operating function

Ownership operator classification permits registration and contracts

Applicable instruments exact versions and source record IDs

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

Applicability decisions exceptions and unresolved questions

Operating technical compliance and project owners with alternates

Decision approvers dates next review and authority record

Field activity authorization worksheet

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

Activity purpose exact targets and asset owners

Method tool version permitted functions and excluded actions

Vendor constraints approved traffic behavior and operating baseline

Operating window communications and named stop authority

Recovery support safe response and resumption authority

Operating approval technical approval date and change record

Evidence and finding worksheet

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

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

Evidence ID source custodian period collection method and integrity

Observed condition and method used to establish it

Applicable requirement exact version and agreed assessment criterion

Operating consequence safeguards assumptions and evidence limits

Finding ID responsible owner priority rationale and challenge

Reviewer disposition date and linked technical record

Corrective action and acceptance worksheet

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

Finding ID action owner dependencies and target date

Approved implementation change record and operating window

Verification criterion authorized method result and evidence IDs

Remaining limitations interim controls and residual risk decision

Operating acceptance compliance disposition and recurring review

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

Technical reviewer sponsor decision date and closure record

Terms used in the planning records

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

Sources

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

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

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

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

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

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

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

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

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

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

W01 AWIA Section 2013 and SDWA Section 1433. EPA. Agency implementation guidance. Covered systems; RRA and ERP content; certification cycles. https://www.epa.gov/waterresilience/awia-section-2013 (checked October 15, 2026)

W02 Certification of Risk and Resilience Assessments and Emergency Response Plans. EPA. Agency implementation guidance. Certification and secure retention of actual plans. https://www.epa.gov/waterresilience/how-certify-your-risk-and-resilience-assessment-or-emergency-response-plan (checked October 15, 2026)

W03 Emergency Response Plan Templates for Drinking Water and Wastewater. EPA. Agency guidance. Separate drinking water and wastewater templates. EPA identifies the wastewater template as voluntary under SDWA 1433. https://www.epa.gov/waterutilityresponse/develop-or-update-emergency-response-plan (checked October 15, 2026)

W10 Wastewater cybersecurity resources. New York DEC. Agency implementation guidance. 6 NYCRR 750-2.7(h) incident reporting within 24 hours and a 30 day report for all SPDES permittees from March 26, 2026; 750-2.9(d) and (e) POTW controls and emergency response plans from March 11, 2027; first certification March 28, 2027. https://dec.ny.gov/environmental-protection/water/water-quality/wastewater-treatment-resources/wastewater-cybersecurity-resources (checked November 3, 2026)

W11 Wastewater cybersecurity regulations compendium. New York DEC. Agency guidance. March 2026 compendium; POTW compliance dates and referenced documents. https://dec.ny.gov/sites/default/files/2026-03/wastewatercyber_compendium.pdf (checked October 15, 2026)

W04 Cybersecurity for Water and Wastewater Facilities. Indiana IDEM. Agency implementation guidance. IC 13-18-16.5; covered facility types; 2026 assessments and incident reporting. https://www.in.gov/idem/cleanwater/cybersecurity-for-water-and-wastewater-facilities/ (checked October 15, 2026)

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

W05 Maryland Environment 9-2705, current selected codified text. Maryland General Assembly. Selected current codified statute. 9-2705(a), (b). Over 3,300 customers for this section. Other Subtitle 27 duties have different scope. Confirm current implementation and reconcile the attachment discrepancy. https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gen&section=9-2705&enactments=false (checked October 17, 2026)

W06 MDE SB871 implementation guidance, May 2026. Maryland MDE. Agency guidance. Sections 3-9; Attachments 1-2. Statute and regulation govern; guidance explains. Attachment 2 people threshold differs from statute customers; confirm current instructions and provider deadlines. https://mde.maryland.gov/programs/water/water_supply/Documents/SB871.pdf (checked October 17, 2026)

W07 Water Quality Accountability Act. New Jersey DEP. Agency implementation guidance. Public community water systems with more than 500 service connections; cybersecurity program; NJCCIC membership and incident reporting. https://dep.nj.gov/watersupply/drinking-water-systems/water-quality-accountability-act/ (checked October 15, 2026)

W08 Water Quality Accountability Act amendments, P.L.2021, c.262. New Jersey Legislature. Enacted law. N.J.S.A. 58:31-2 (more than 500 service connections), 58:31-4.1 (program covering all industrial control systems), 58:31-4.2 (prompt NJCCIC reporting; NJCCIC audit within 30 days). https://pub.njleg.gov/bills/2020/PL21/262_.HTM (checked November 3, 2026)

W09 New York drinking water cybersecurity applicability. New York DOH. Current rule page. 10 NYCRR Appendix 5-E: community water systems serving more than 3,300 people. https://regs.health.ny.gov/content/section-5-e1-applicability (checked October 15, 2026)

S25 Missouri starting source. Missouri Legislature. Codified sector clause. Section 640.142 requires a cyberrisk plan including assessments and controls. Exemptions include systems without internet connected controls; state parks; cities above 30,000 inhabitants; specified charter county population bands; and PSC regulated utilities above 30,000 customers. Document every exclusion and actual entity facts. No assessment frequency or pentest requirement is supplied by this section. https://revisor.mo.gov/main/OneSection.aspx?section=640.142 (checked October 17, 2026)

S29 New Hampshire starting source. New Hampshire Legislature. Enacted sector law. State authority and applicability sources current to October 15, 2026. https://gc.nh.gov/rsa/html/L/485/485-3-e.htm (checked October 15, 2026)

NH-WW Wastewater cybersecurity protection program. New Hampshire Legislature. Enacted sector law. RSA 485-A:5-f; current codified text. https://www.gc.nh.gov/rsa/html/L/485-A/485-A-5-f.htm (checked October 15, 2026)

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

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

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

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

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

Plan the assessment with a senior examiner

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

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

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

Request a consultation online at evestigate.com/contact.

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