Water and Wastewater OT Manual for Assessing Without Touching Setpoints

Edition November 18, 2026

New York water summaries, PSC test acceptance and the PSC adoption source were checked on November 18, 2026. Unrelated authorities retain their earlier verification dates.

This water assessment manual explains how to examine operational controls while preserving the plant's operating authority. Read the procedures here, record the work in the editable worksheets and use the matching PDF when a printed reference is more useful.

Planning scope and research basis

This manual is built for a controlled assessment of treatment, disinfection, pumping, storage, distribution, collection and effluent control at systems in the United States. It carries the federal drinking water and wastewater research; the companion volume screens all fifty states so you can resolve the state cybersecurity statutes, permit conditions and local ownership questions that decide what your system actually owes.

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 printable worksheets carry the work from planning through handover, and the applicability register begins with the PWSID, the permit and the population served because every later duty is counted from them.

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 utility's own permits, certification receipts and state correspondence are the first records the assessment requests.

Open applicability

The source register sorts binding instruments, guidance, drafts, superseded versions and open questions into their own entries. Each open entry names the controlling text and the facility facts to gather, and the site specific conclusion is signed once they are in the record.

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

Adoption and review

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

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-82 Rev. 4 initial public draft, Guide to Operational Technology (OT) Security (F02), A survey of cyber security management in industrial control systems (R01), Threat modeling of industrial control systems: A systematic literature review (R02), ICSSIM: A framework for building industrial control systems security testbeds (R03)

Tell a senior examiner the PWSID, the population served and the remote sites, and the first scoping conversation will sort out which records the register needs.

Indiana and Maryland Water Thresholds

Indiana and Maryland count their water cybersecurity duties differently, and a utility in either state sets its calendar from these thresholds.

Indiana and Maryland

For Indiana, IDEM currently identifies an annual vulnerability assessment, certification by December 31 2026 and every other year thereafter, and annual reporter designation before September 1. The Indiana row is signed once the current IC 13-18-16.5 text, the approved tools, the actual scope and the independent incident triggers are confirmed. For Maryland, the current Environment 9-2705 applies to community water and sewerage systems serving over 3,300 customers, with a maturity assessment by July 1 2026 and every two years. Record the all system contact, training and reporting duties and the state office collection dates in their own rows, apart from the operator's own filing duties. The May 2026 MDE guidance supplies submission instructions, but its Attachment 2 counts people where the statute counts customers.

Preparation workflow

Use the Assessment prep worksheet and its CSV to prepare audits, cyber and physical assessments and penetration tests. Gather the permissions, the third party authority, the OT safety restrictions, the stop and recovery arrangements and the existing evidence first, and then agree the method. Use the State research checklist, one row per state and sector, to assign further state and sector research alongside the local, operator, permit and client facts.

Evidence and implementation

The May 2026 MDE guidance now describes secure MoveIT submission. Its Attachment 2 uses people rather than statutory customers. Record the conflict in the applicability register, confirm current account eligibility and filing instructions with the agency, and close the row with the agency's own answer.

Sources: IDEM Cybersecurity for Water and Wastewater Facilities (W04), Maryland Environment 9-2705, current selected codified text (W05), MDE SB871 implementation guidance, May 2026 (W06)

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

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 filled is a result, a row still being filled is a plan, and the workbook keeps the two visibly apart.

Pre Execution Readiness Checklist

Fill the criterion, population, period and sampling rationale first, ahead of any system work, 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 permit and rule citations stay distinct from the operators' approvals.

Pending Scope and Governance Decisions

The open count on the Start sheet counts blank decisions, decision text that needs correcting and resolved selections that need a required record field. Treat Fields present as the prompt for qualified review, which is the step that completes the row. The responsible operating, technical and compliance people sign 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 a facility conclusion when the controlling instrument is recorded beside it. For New York work use the Clause matrix and questions Q01 to Q10 in the New York set. Current instruments and local facts that are still being gathered carry the Unresolved status, which clears when someone retrieves the text or establishes the fact.

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 come to it, and keep the duty on the register while the text arrives. Use the Edition record to track your own revisions and reviews, and keep the previous version when you adopt a new one.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

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

Using this planning pack

Use this pack in the order a utility makes decisions. Fix the legal and operating boundary first, because the PWSID, the population served, the permit and the ownership of each remote site decide which duties attach to treatment, disinfection, pumping, storage, distribution, collection and effluent control. Choose evidence and methods once the operators responsible for the process have agreed what may be examined, so the assessment works alongside safe water operations.

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. 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 first, then schedule 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 has a later compliance date, and an approved standard can reach enforcement at a later date. Record both dates and the applicable version, and take each deadline from the instrument's effective date.

Signing an assessment conclusion

The reviewer signs against the actual facility facts, the current instruments, the examined evidence, the test permissions and the open questions recorded with them. Preparing this pack readies the facility, and the assessment itself is the examination that follows. A named technical reviewer reviews the completed work, and the organization then adopts or publishes its conclusions.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

Agreement with the operators on what may be examined comes first, ahead of any method; (800) 868-8189 reaches examiners who hold that conversation with operations first.

Decisions before mobilization

Distinguish community drinking water systems, noncommunity water systems, publicly owned treatment works, private wastewater facilities and industrial dischargers as the first step, ahead of any checklist, because each carries different federal and state duties. Record population served, service connections and customers as three separate quantities with their own evidence, since different states measure coverage with different units, and keeping each figure distinct lets the utility state its own applicability accurately.

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

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 at the outset, so any description of the work as independent sits beside a recorded disclosure.

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 the identity, DNS, time, virtualization, telecommunications and backup dependencies whose failure could affect the process, because the record follows the process past the controller to the services that can actually take it down. Identify shared corporate services and third party interfaces explicitly, and record test permission for each as its own decision, so the scope names them and the permit governs them. 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.

Record each exclusion and its effect

Document every excluded safety system, vendor appliance outside reach, firmware past vendor support, protocol outside the approval and record held elsewhere, and state in one sentence how each exclusion shapes the conclusion. An excluded critical dependency stays in the report as a visible item the sponsor accepted. Fixing the asset count at the start keeps the scope matched to the process rather than to convenience.

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 approval is that signed, dated entry itself.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

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, and three authorities stay explicit at every team size: who authorizes operating activity, who reviews evidence, and who accepts residual risk.

Sponsor or CISO

Role: Sponsor or CISO

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

Decision or work owned: 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

Role: Operating owner and engineering authority

Decision or work owned: 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 remain under operations control throughout the assessment.

Compliance and legal owners

Role: Compliance and legal owners

Decision or work owned: Resolve the applicable instruments, disclosure restrictions and incident reporting duties. Identify the responsible filing official and an alternate who acts in the official's absence.

Technical lead and field technician

Role: Technical lead and field technician

Decision or work owned: Design the permitted method and collect traceable evidence. A technician works to the permitted target list and tool settings, and an active test goes ahead on the written authorization of the people named in the permit.

Project manager

Role: Project manager

Decision or work owned: 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

Role: Evidence custodian and quality reviewer

Decision or work owned: Control evidence access, integrity, retention and the independent review of facts and conclusions. Record conflicts of interest and review exceptions.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

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.

1 Applicability and scope

Stage: 1 Applicability and scope

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

Required exit evidence: 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

Stage: 2 Readiness

Required exit evidence: Approved evidence request, interview schedule, collection method, secure workspace, current backup evidence and operating contacts with alternates.

3 Examination

Stage: 3 Examination

Required exit evidence: Asset and process records, reconciled diagrams, sampled control evidence and a dated account of what was examined and what was held outside the examination.

4 Authorized validation

Stage: 4 Authorized validation

Required exit evidence: Activity permits, baseline observations, test log, stop and recovery record and post work operating acceptance. The record states whether validation was authorized and the reason for that decision.

5 Reporting and decisions

Stage: 5 Reporting and decisions

Required exit evidence: Reviewed findings, requirement mappings, stated boundaries, corrective owners, funding decisions and a residual risk record signed by the person entitled to accept it.

6 Verification and handover

Stage: 6 Verification and handover

Required exit evidence: Retest evidence, recurring review schedule, retained records, lessons and a signed handover. A recommendation closes when it is verified or formally dispositioned.

Sources: NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

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 one row per obligation 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.

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

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 on the register 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, 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 where that answer lives.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), CIRCIA public rulemaking notice (F05), Cybersecurity Resource Center (F09)

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. Wastewater systems are screened under their own state and permit instruments, and the first entry in the water applicability register is the population figure and the evidence behind it.

Scope and content

Record each PWSID, its community system status and its population served. The complete RRA extends well beyond cyber risk and includes physical systems, monitoring, financial infrastructure, chemicals and operation and maintenance. Map the cyber evidence into the complete RRA as one contribution to the statutory assessment; a regulator reviewing the certification will look for the whole document.

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 rather than the intended date. ERP certification is due within six months of the actual RRA certification, which can fall earlier than the 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. Where a receipt is missing, reconcile it now against the actual RRA certification, which remains the date the six month ERP period runs from. The subsequent five year review and certification duties need their own calendar rows.

Evidence and filing

Retain the completed RRA, the ERP, the cyber contribution, the approved revisions, the certification statements and the acknowledgments. EPA instructs utilities to submit certifications rather than the plans themselves and to keep the plans securely for at least five years, so the controlled record holds both the plan and the proof of submission. Coordinate with the local emergency planning committee to the extent possible, as the program requires.

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

Sources: AWIA Section 2013 and SDWA Section 1433 (W01), Certification of Risk and Resilience Assessments and Emergency Response Plans (W02)

Wastewater and discharge obligations

Treat wastewater facilities as their own regulated population. State law and the facility permit can impose cyber duties on their own authority, independently of AWIA, and the permit is the instrument the assessment reads first.

Establish the permit boundary

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

Connect cyber events to physical reporting

An unauthorized account event and a sewer overflow trigger different reporting duties, and a single incident can trigger both. Evaluate the cyber event and the process consequence on separate clocks. Obtain the current permit and the state instructions for notification timing, channel and follow up. The permit clock runs from awareness, and attribution follows on its own timeline.

New York example

All SPDES permittees, public or private, report a cybersecurity incident meeting 750-1.2(a)(27) to the Regional Water Engineer orally as soon as possible and no later than 24 hours after becoming aware of it, followed by the written report within 30 days of awareness under 750-2.7(h). These duties took effect March 26, 2026. Current DEC instructions require the initial online incident report followed immediately by oral notification to the regional water engineer or manager; use DEC Dispatch if the regional contact cannot be reached. Record awareness, the affected operations or SPDES data, notification times, the written report and receipts separately from the DOH and PSC records.

Operational evidence

Trace the collection and treatment alarms, the telemetry dependencies, the pump controls, the disinfection and the effluent monitoring. Examine how personnel detect loss of visibility, verify actual conditions, contact the permit authority and maintain an approved safe operating response, and ask for the last occasion on which they did so. EPA's wastewater ERP template is useful voluntary guidance, and SDWA 1433 certification remains a drinking water duty.

Sources: Emergency Response Plan Templates for Drinking Water and Wastewater (W03), NYSDEC wastewater cybersecurity resources (W10), Wastewater cybersecurity regulations compendium (W11)

State water requirements that change the plan

Use the fifty state companion for every facility. The examples below each use a different population unit and a different schedule, and the planning action names the record that settles applicability.

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

Indiana W04

State and source: Indiana W04

Planning action: Screen covered computerized or SCADA facilities, including the specified community water and wastewater categories. Verify the 500 person water threshold. Separate the annual assessment by December 31 from 2026, the certification every other year from December 31 2026, and the annual August 31 reporter designation.

Maryland W05 W06

State and source: Maryland W05 W06

Planning action: Use more than 3,300 customers under Environment 9-2705 for the enhanced scope. Confirm the July 1 2026 maturity assessment and the two year cycle. Reconcile the agency's certification collection with the actual operator submission instructions.

New Jersey W07 W08

State and source: New Jersey W07 W08

Planning action: Use more than 500 service connections for WQAA scope. Check the annual controls assessment and certification, the framework updates and the incident obligations. Confirm any separate BPU order and the broader incident reporting law.

New York drinking water and wastewater

State and source: New York drinking water and wastewater

Planning action: Use the New York water duties section in this edition. It separates DOH and DEC scope, reporting triggers, controls, recurring reviews and certification roles. Water requirements contains one record per duty rather than a combined state prompt.

Missouri S25 and New Hampshire S29 NH-WW

State and source: Missouri S25 and New Hampshire S29 NH-WW

Planning action: Evaluate the statutory Internet connected control exemptions and the other stated exceptions.

Sources: IDEM Cybersecurity for Water and Wastewater Facilities (W04), Maryland Environment 9-2705, current selected codified text (W05), MDE SB871 implementation guidance, May 2026 (W06), NJDEP Water Quality Accountability Act (W07), Water cybersecurity amendments (W08), New York drinking water cybersecurity applicability (W09), NYSDEC wastewater cybersecurity resources (W10), Wastewater cybersecurity regulations compendium (W11), RSMo 640.142 (S25), N.H. RSA 485:3-e (S29), NH-WW Wastewater cybersecurity protection program

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

New York Water Duties and the Evidence to Keep

Confirm the system and the governing rule

Begin with the system type, public water system identifier or SPDES permit, population served, combined wholesale and retail population, ownership and treatment design flow. Appendix 5-E generally covers community drinking water systems serving more than 3,300 people. Its personnel and network logging provisions use a combined wholesale and retail population greater than 50,000. All Subpart 5-4 certified drinking water treatment operators have the training duty, regardless of system size. Examine each exclusion against the actual architecture; an exclusion can leave incident reporting and response planning duties in place.

Designate the responsible person

For a covered system serving a combined wholesale and retail population greater than 50,000, subject to applicable exclusions, the owner designates a person with demonstrable cybersecurity knowledge and practical system protection or risk management experience. Section 5-E.4 does not require a professional cybersecurity certification. Record the designation, qualifications and contact in the emergency plan. That person reports confidentially to the governing body at least annually and submits the separate program compliance certification required by 5-E.6(b) with the emergency plan submission.

Keep the DOH reporting clocks separate

For a covered system, report to DOH as soon as possible and no later than 24 hours after determining that a cybersecurity incident as defined in 5-E.3(e) has occurred which has created or may create a public health hazard. Separately, vulnerabilities identified in the cybersecurity vulnerability analysis that may affect compliance with Subpart 5-1, or any situation that may pose a public health risk, must be reported within 48 hours of identification under 5-E.1(c)(2) and 5-E.5(e). Record each qualifying condition, its timestamp and the receipt. Other applicable State and Federal notices retain their own triggers.

Plan the recurring drinking water work

The remaining Appendix 5-E requirements have a January 1, 2027 compliance date; operator training and incident reporting took effect on adoption on March 11, 2026. Complete the cybersecurity vulnerability analysis using the DOH approved form, obtain the required approval and incorporate its findings into the emergency plan. Review and update the analysis at least annually and within 30 days after major water facility infrastructure changes become operational. The cybersecurity program follows those findings. Use the detailed Water requirements and Water tests records to examine each applicable program provision separately.

Correct significant deficiencies on the required schedule

When the State notifies the system of a significant deficiency, consult the State within 30 days. Within 120 days of that notification, or an earlier period directed by the State because of a public health threat, correct the deficiency or comply with the applicable corrective action plan under 5-1.71(c) and (d). Opening a work ticket does not establish that condition. Keep the approved schedule, progress and completion evidence together. Public health hazards require the State directed or approved action and the applicable Tier 1 public notice.

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

Report wastewater incidents from awareness

All SPDES permittees, public or private, report a cybersecurity incident meeting 750-1.2(a)(27) to the Regional Water Engineer orally as soon as possible and no later than 24 hours after becoming aware of it, followed by the written report within 30 days of awareness under 750-2.7(h). These duties took effect March 26, 2026. Current DEC instructions require the initial online incident report followed immediately by oral notification to the regional water engineer or manager; use DEC Dispatch if the regional contact cannot be reached. Record awareness, the affected operations or SPDES data, notification times, the written report and receipts separately from the DOH and PSC records.

Prepare the POTW controls and response plan

Publicly owned treatment works must meet the cybersecurity control and emergency response plan requirements in 750-2.9(d) and (e) by March 11, 2027. The first annual certifications are due March 28, 2027. Network monitoring and logging under 750-2.9(e)(2) applies at a design flow of at least 10 million gallons per day, with the rule's exceptions for no physical or logical OT connections to IT or external networks, or solely devices capable only of one way traffic from OT. Other POTW duties still require their own assessment. Use the incorporated documents and specified editions listed in the rule, alongside separately identified guidance.

Confirm who can sign the wastewater certification

The municipal principal executive officer or ranking elected official signs the certifications, or a duly authorized executive level municipal official with the required oversight signs under the rule's written authorization provisions. Submit that authorization to DEC. A consultant's engagement does not itself confer filing authority. Retain the evidence supporting the signed certifications and the annual filing receipts.

Follow the evidence through to verification

Use Water requirements for one record per duty, Water tests for the criterion and safe examination procedure, Water reporting for the separate clocks, and Water calendar for recurring work. Establish applicability before assigning a conclusion. Each result names its evidence, examiner, operating permission and reviewer. A completed record leads to a supported finding, corrective work and a separate retest. The New York water toolkit includes manager, operator and governing board guidance and two completed fictional examples.

Open the New York water toolkit and completed examples.

Sources: NYSDOH Appendix 5-E: Cybersecurity Requirements for Public Water Systems (NYDOH-APP5E, Sections 5-E.1 through 5-E.11); NYSDOH Subpart 5-1: Public Water Systems (NYDOH-SUBPART51, Sections 5-1.33, 5-1.71 and 5-1.77; agency compilation revised October 8, 2026); NYSDEC adopted revised Part 750 express terms (NYDEC-750-2026, 750-1.2(a), 750-1.25(j) through (o), 750-2.7(h), 750-2.9(d) through (f)); NYSDEC Wastewater Cybersecurity Regulations: Compendium of Resources (NYDEC-COMPENDIUM, Pages 2 through 24 and regulatory appendices); NYSDEC Wastewater Cybersecurity Resources (NYDEC-IMPLEMENTATION, Effective dates, applicability, reporting, plans, training and annual certification questions).

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

Water process examination

Build separate evidence paths for safe treatment, distribution continuity and wastewater consequences. Each path starts at the physical measurement the operator trusts and works back to the controller and the network that could alter it.

Treatment and dosing

Identify how approved chemical setpoints, recipes and control logic are established, changed, checked and restored, and request the controller project files with their change history. Examine the access approvals and the change evidence. Ask operations how an incorrect value would be detected by independent measurement or operator checks, and record the answer with the instrument that provides the independent reading.

Remote pumping and telemetry

Record the communications ownership, the remote asset access, the loss of communications behavior, the operator alarms, the local operating capability and the physical access at each remote site. Ask for one representative current communication loss or recovery record; most utilities hold one, and the examiner reads it for how the site actually responded. Any live interruption or controller failover requires a separately approved operating test.

Laboratory and reporting interfaces

Trace the data used to make treatment, public health and discharge decisions from the instrument to the report. Review access, time integrity, retained records and the exceptions used when data is unavailable or unreliable. Establish who can validate field measurements and who can 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 its safeguards. Where process interlocks, manual operation or alarm effectiveness were described in interviews, the finding records them as described, and it records as demonstrated only what was shown, in those words.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), AWIA Section 2013 and SDWA Section 1433 (W01), Emergency Response Plan Templates for Drinking Water and Wastewater (W03)

Water incident and continuity exercise

Use an exercise to test decisions and records while the live process runs untouched. The following scenario is fictional, and it is built around the vendor account and the remote site that most utilities monitor least.

Scenario

A vendor account is suspected of unauthorized access to a remote pumping environment. Telemetry values are inconsistent, and the operators are still confirming the actual process condition. An operator also reports a communications alarm.

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

Controller prompts

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

Test the decisions

Record the first awareness timestamp, the event classifications, the alternate communications, the credentials held securely, the supplier reachability and the 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, because an ERP kept in a copy the team can reach during an outage is the one that serves the incident it was written for.

Acceptance and correction

The observer records the decisions, the supporting evidence, elapsed times where they were measured, the contacts to add and the assumptions to correct. Assign an owner to every open issue. A tabletop result demonstrates the decision process, and the plant restore and the regulator's acceptance are each confirmed by their own records.

Sources: NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04), Emergency Response Plan Templates for Drinking Water and Wastewater (W03), NYSDEC wastewater cybersecurity resources (W10)

Water reporting and recurring calendar

Populate the calendar from signed applicability decisions and actual prior completion records rather than from intended dates. Each row names the trigger and the evidence that records the duty was met.

AWIA RRA and ERP

Record: AWIA RRA and ERP

Trigger and evidence: Track each PWSID, its population cohort, the actual certification dates, the ERP dependency and the five year review cycle. Retain acknowledgments and the current plans.

State program

Record: State program

Trigger and evidence: Record the applicable annual or two year assessment, certification, training and framework update duties separately.

Operational event

Record: Operational event

Trigger and evidence: Use the current permit and the state definition for treatment failure, loss of safe service, bypass, overflow or discharge. Record the separate initial and written follow up clocks.

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

Cyber incident

Record: Cyber incident

Trigger and evidence: For applicable Indiana facilities, IDEM identifies 24 hours after discovery when operations are affected and two business days when they are not. Check the current reporting instructions and any concurrent public entity duties.

Physical and organizational change

Record: Physical and organizational change

Trigger and evidence: Review whether the change triggers a new analysis, a plan revision, a regulator notice or a recertification. Keep the change decision and the source that establishes the trigger together.

Sources: AWIA Section 2013 and SDWA Section 1433 (W01), Certification of Risk and Resilience Assessments and Emergency Response Plans (W02), IDEM Cybersecurity for Water and Wastewater Facilities (W04), Maryland Environment 9-2705, current selected codified text (W05), MDE SB871 implementation guidance, May 2026 (W06), Water cybersecurity amendments (W08), New York drinking water cybersecurity applicability (W09), NYSDEC wastewater cybersecurity resources (W10)

Document requests and interviews

Request existing records first, ahead of any proposal for 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 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 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 allow a supervised on site review for any record that stays at the facility. Record each item still outstanding 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 usually are 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 remote stations speaks for the remote stations, and the report states both the sample and the population outside it in plain terms.

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 every interview statement is recorded as a statement and every tested fact as a tested fact.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

Safe work and stop authority

Water operations determine safe treatment, pressure, chemical dosing and discharge conditions. Every setpoint, dosing rate, alarm limit and controller mode stays in the hands of operations. 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 qualified plant staff who hold those programs. Verify the asset owner, the permitted access point, the device approval, its malware screening, the cable path and the isolation design, and then attach the collection device. 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 treatment, disinfection, pumping, storage, distribution, collection and effluent control. 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, and isolation, device resets and process restarts all happen at that owner's 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. Hold the activity permit while operations and the technical lead review the cause, then reauthorize the changed method and the remaining targets. A stop that is logged and reviewed is a mark of a controlled assessment, and the log is the record a later reviewer reads to confirm the assessment was run that way.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), State Plans (F06)

Inventory and process dependencies

Build an inventory that explains how each asset supports treatment, disinfection, pumping, storage, distribution, collection and effluent control. An inventory ties each address to its function, and a passive discovery export joins it once it has been reconciled against the drawings.

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 loss of treatment control, unsafe chemical dosing, loss of distribution pressure, sewer overflow or impaired effluent monitoring. 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 is recorded as independent when engineering has shown how it is isolated, whatever layer of the drawing it sits 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 gets its own control and recovery decision, and patching, scanning or replacing it during the assessment is an operating decision that operations approves. Expect the first reconciliation to surface undocumented engineering laptops, dual homed workstations and vendor modems; those are findings, and the inventory is where they belong.

© 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 high consequence dependency still open. Sensitive addressing and configuration detail belong in the controlled technical appendix, and the management report carries the summary.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), A survey of cyber security management in industrial control systems (R01), Threat modeling of industrial control systems: A systematic literature review (R02)

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 test is where a segmentation claim is 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 an installed controller supports a narrower mechanism, evaluate the controls at an approved access gateway and say so in the finding. The examiner looks closely at three common 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, a separate authorized activity with its own permit, tests whether the path is reachable. A proposed segmentation improvement moves from recommendation to verified as it is implemented and tested, 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, a conformity statement is made against the licensed edition and the agreed assessment criteria. The publicly described zone and conduit approach is a design method, and the assessment uses it to read the architecture.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), ISA/IEC 62443 Series of Standards (F08)

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 constraint, 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. A shared operator account still on its commissioning password is common, 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. When a controller answers a scan slowly, the team pauses and reviews 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 contract promises that practice has yet to match and dependencies awaiting a named owner. Include a supplier contact and an escalation alternate in the operating handover so the operator reaches support during an incident in one call.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), ISA/IEC 62443 Series of Standards (F08)

© 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, leave production clocks as they run, and translate timestamps in the analysis.

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 itself is 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 records 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 the other side in a dispute, 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: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04)

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. A successful backup job records that a file was written, and a representative restore is where recovery is demonstrated.

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

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 an incident, and whether the engineering software has a copy apart from the workstation an attacker would target. 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 carries the work wherever operations judge production unsuitable.

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 demonstrates a decision process, a technical restore is demonstrated on its own, 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 actually measured, the open dependencies and the corrective owner. Operations accepts the restored state. Assumptions awaiting a test stay explicit in the report and are scheduled in the recurring program.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04), ICSSIM: A framework for building industrial control systems security testbeds (R03)

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.

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

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: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), ICSSIM: A framework for building industrial control systems security testbeds (R03)

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, because a reviewer gives each its proper weight when the two are kept apart.

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 what it covers. 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 when the evidence points to a condition the examination has yet to confirm. Record recommendation, implementation and verification as three separate states. A screenshot of a changed configuration supports implementation.

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

Prioritize consequence and confidence

Evaluate the potential effects on treatment, disinfection, pumping, storage, distribution, collection and effluent control, the exposure paths, the existing safeguards, the recovery capacity and the 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, 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 risk method: record that method and its acceptance authority, and keep the plant score grounded in it rather than in multiplied numbers.

Resolve challenge

Give the operating owner a documented opportunity to identify asset facts to correct, safeguards to add and remediation proposals to revise for safety. 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 report delivery date.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), A survey of cyber security management in industrial control systems (R01), Threat modeling of industrial control systems: A systematic literature review (R02)

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, which is what turns a scan export into work an owner 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 carry the Deferred label on a postponed action through to 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 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.

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

Regulatory conclusion

State the obligations actually assessed, with their versions, the facility scope, the sample and the dates, and list in their own section the requirements outside this assessment and those awaiting demonstration.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

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 cue to schedule verification, and the verified control result comes from that check.

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, when the corporate document system may be the thing that is down. 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, then set the 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: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04)

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

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.

Evidentiary Record Fields

Field activity authorization worksheet

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

Evidentiary Record Fields

Evidence and finding worksheet

Record facts separately from possible consequences. Link the original evidence, preserve the source times and state the scope of each method, so a reviewer working from the record alone can reproduce the finding.

Evidentiary Record Fields

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

Terms used in the planning records

OT ICS and SCADA

Term: OT ICS and SCADA

Meaning in this pack: Operational technology; industrial control systems; supervisory control and data acquisition.

PLC RTU HMI DCS SIS

Term: PLC RTU HMI DCS SIS

Meaning in this pack: Programmable logic controller; remote terminal unit; human machine interface; distributed control system; safety instrumented system.

RRA ERP and PWSID

Term: RRA ERP and PWSID

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

Meaning in this pack: Risk and resilience assessment; emergency response plan; public water system identifier.

BES CIP DER and EMS DMS

Term: BES CIP DER and EMS DMS

Meaning in this pack: Bulk Electric System; Critical Infrastructure Protection; distributed energy resources; energy/distribution management system.

SSI CEII and CUI

Term: SSI CEII and CUI

Meaning in this pack: Sensitive Security Information; Critical Energy/Electric Infrastructure Information under the applicable authority; Controlled Unclassified Information. Determine the actual handling regime.

CySO CISO and EHS

Term: CySO CISO and EHS

Meaning in this pack: Cybersecurity Officer; Chief Information Security Officer; environment health and safety.

PHA MOC and CMMC

Term: PHA MOC and CMMC

Meaning in this pack: Process hazard analysis; management of change; Cybersecurity Maturity Model Certification.

Applicable and Unresolved

Term: Applicable and Unresolved

Meaning in this pack: Applicable requires facility facts and a controlling instrument. Unresolved identifies a fact or authority still being gathered, and it keeps the row open on the register, distinct 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, with current law and effectiveness figures taken from the primary sources.

© 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, which the assessment applies to the specific plant.

R03 ICSSIM A framework for building industrial control systems security testbeds

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

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-82 Rev. 4 initial public draft, Guide to Operational Technology (OT) Security (F02), A survey of cyber security management in industrial control systems (R01), Threat modeling of industrial control systems: A systematic literature review (R02), ICSSIM: A framework for building industrial control systems security testbeds (R03)

Sources F03 to W02, federal guidance and water and wastewater instruments

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; its reporting clocks begin on the effective date the Federal Register publishes, so check the Register when setting the calendar.

F09 Cybersecurity Resource Center

New York DFS. Agency implementation source. 23 NYCRR Part 500 covered entity scope. Covered entity status is decided under the Part 500 definition, which the register checks for each New York operator apart from its location.

W01 AWIA Section 2013 and SDWA Section 1433

EPA. Agency implementation guidance. Covered systems; RRA and ERP content; certification cycles.

W02 Certification of Risk and Resilience Assessments and Emergency Response Plans

EPA. Agency implementation guidance. Certification and secure retention of actual plans.

Sources: NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), CIRCIA public rulemaking notice (F05), Cybersecurity Resource Center (F09), AWIA Section 2013 and SDWA Section 1433 (W01), Certification of Risk and Resilience Assessments and Emergency Response Plans (W02)

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

Sources W03 to W05, water and wastewater instruments

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.

W10 Wastewater cybersecurity resources and adopted rules

New York DEC. Agency implementation guidance. 6 NYCRR Parts 616 650 and 750; March 2026 adoption; reporting.

W11 Wastewater cybersecurity regulations compendium

New York DEC. Agency guidance. March 2026 compendium; POTW compliance dates and referenced documents.

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.

W05 Community Water and Sewerage System Cybersecurity

Maryland General Assembly. Current selected Environment 9-2705; over 3,300 customers for that section. Other Subtitle 27 duties and actual implementation each receive their own review.

Sources: Emergency Response Plan Templates for Drinking Water and Wastewater (W03), NYSDEC wastewater cybersecurity resources (W10), Wastewater cybersecurity regulations compendium (W11), IDEM Cybersecurity for Water and Wastewater Facilities (W04), Maryland Environment 9-2705, current selected codified text (W05)

Sources W06 to S25, water and wastewater instruments and state authorities

W06 Guidance on Senate Bill 871

Maryland MDE. May 2026 SB871 implementation guidance, sections 3-9 and Attachments 1-2. Secure submission instructions now exist. Attachment 2 uses people instead of statutory customers; confirm current provider timing and scope with MDE.

W07 Water Quality Accountability Act

New Jersey DEP. Agency implementation guidance. Cybersecurity plans; annual assessment; scope over 500 service connections. Read alongside chapter law W08.

W08 Water cybersecurity amendments

New Jersey Legislature. Enacted chapter law. P.L. 2021, c. 262 and N.J.S.A. 58:31-4.1.

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

W09 New York drinking water cybersecurity applicability

New York DOH. Department hosted rule text. Appendix 5-E.1 through 5-E.11. The scoped New York water duties section and its source register distinguish exclusions, immediate training and reporting duties, and the January 1, 2027 transition.

S25 Missouri selected authority

Missouri Legislature. Selected enacted sector law. Selected state authority and applicability, reviewed October 16, 2026.

Sources: MDE SB871 implementation guidance, May 2026 (W06), NJDEP Water Quality Accountability Act (W07), Water cybersecurity amendments (W08), New York drinking water cybersecurity applicability (W09), RSMo 640.142 (S25)

Sources S29 to F08, federal guidance and state authorities

S29 New Hampshire selected authority

New Hampshire Legislature. Enacted sector law. Selected state authority and applicability, reviewed October 16, 2026.

NH WW Wastewater cybersecurity protection program

New Hampshire Legislature. Enacted sector law. RSA 485-A:5-f; current codified text.

F04 Incident Response Recommendations and Considerations Revision 3

NIST. Final guidance. April 2025 final publication.

F06 State Plans

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

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 is made against the licensed edition the organization holds.

Sources: N.H. RSA 485:3-e (S29), NH-WW Wastewater cybersecurity protection program, NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04), State Plans (F06), ISA/IEC 62443 Series of Standards (F08)

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