New York Water Cybersecurity Toolkit

Edition November 18, 2026

Know what is due. Know what to do next. Your water system needs a clear work plan, records that stand up to review and people who know what they are responsible for. Use this toolkit to identify the New York requirements to examine, organize the evidence and give managers, operators and governing boards a practical next step.

Start With Your System

Edition November 18, 2026. This toolkit organizes the New York drinking water and wastewater work identified in its authority register, with separate federal water references where relevant. PSC, DFS, private information, other permit conditions and other jurisdictions need their own applicability reviews. Unknown facts remain unresolved. Source verification dates describe when the material was checked and do not claim agency review, owner approval of this preview or endorsement of a utility's compliance. The two worked examples are fictional teaching records.

Identify the system and the responsible people

Use the first working session to establish what you operate, the legal owner, the relevant system or permit identifier and the person coordinating this work. Locate the public water system record or SPDES permit, the current assessment and plans, and the contact register. Record document versions and owners. An unanswered question stays visible until the appropriate person resolves it.

Choose the track from documented facts

Drinking water, wastewater and other utility duties have different coverage tests. Record population, service connections and design flow in their correct units. Use the requirement register to make a supported applicability decision, retaining the decision maker and date. If a fact is missing, mark the decision unresolved rather than excluding the duty. Keep PSC, DFS and private information reviews separate from the water tracks.

Leave the first hour with a useful work plan

Assign a coordinator, select the water track, identify the nearest duties and name the people who can provide the first records. Enter each missing record or decision beside its requirement identifier. Separate a legal deadline or event trigger from the team's proposed completion date. The first session should produce owners and next actions, even when the evidence is not yet complete.

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

Read the authority and the evidence differently

A binding rule states a duty. An incorporated document supplies provisions made applicable by that rule, in the specified edition. Agency guidance explains implementation; a recommended practice supports the assessment without becoming a duty merely because it appears in this toolkit. Facility evidence records what your system actually has or does. Keep these source types distinct and use the cited section to identify the criterion for each examination.

Use the same edition throughout the work

Read the guide online, print the PDF for a working session, or use the editable workbook and CSV to assign owners and track records. Retain the edition and requirement identifiers with completed work. Keep facility evidence in the location approved by your organization and enter references to those records in the work plan. Core files can be used without submitting a completed security worksheet.

Begin with existing records and authorized demonstrations. Technical testing, configuration changes and connections to operating systems require the plant's permission, an agreed method and the responsible operational personnel. Keep plant diagrams, credentials and detailed weaknesses in the organization's approved evidence store. Use the initial consultation request to describe the service and help needed, then arrange a suitable transfer method for sensitive material.

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

Give Every Task an Owner and a Clear Finish

A useful plan identifies the applicable duty, the person responsible, the evidence needed, the date that matters and the condition that would support closure. Begin with time sensitive reporting duties and required plans, then work through the detailed records. Keep a regulator's deadline separate from the date your team proposes to finish the work.

Agree on scope and operating authority

Confirm the systems, locations and period to be examined with the operational owner. Record the approved evidence method and any access limits. A consultant's technical recommendation still needs the utility's decision about staffing, operating windows and authority to proceed.

Assign work against a requirement

For each applicable requirement, record its identifier, why it applies, the work to complete, the accountable owner, evidence references, legal date or trigger, project target, current result and next action. Retain a supported exclusion with its reason and reviewer. An unresolved fact is not an exclusion.

Distinguish progress from verification

Use results that describe the evidence: Not examined, Evidence insufficient, Gap identified, Corrective work in progress, or Verified for the stated scope. Receiving a document or completing a template does not by itself verify a control. A corrected record or configuration needs a separate check before the finding is closed.

Prepare the next decision

Bring unresolved requirements, located records and decisions requiring approval to the assessment discussion. Identify who will authorize technical work and who will sign any applicable filing. Keep resources, operating approvals and evidence gaps explicit so the next meeting can resolve something concrete.

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

Make the Operator's Next Step Clear

Provide reliable operating context and evidence without putting treatment at risk. Start with existing records and an authorized demonstration. Leave changes to equipment, access controls and live systems to the responsible technical team under the plant's approval process.

Confirm what the assessment covers

Compare the assessment scope with the current asset list, operational locations and approved system diagram. Ask the technical owner to explain a remote site, vendor access path or supporting service that does not appear in the assessment. Record the versions examined and the specific question still open. Useful evidence includes a dated asset register and scope cross reference. The task is complete when the reviewer can account for the selected population and explain its limits; unexplained omissions remain open.

Check the approved access route

Ask the technical owner to demonstrate the authorized remote access process using a safe account and the approved review method. Compare the observed route and authentication settings with the applicable criterion and approved procedure. Retain the access approval, configuration reference and observation record, including who demonstrated the process and when. Do not attempt a new connection to a controller or change an access rule through this worksheet. State which route was examined and which conditions were not examined.

Make the response plan usable

Locate the approved plan, controlled copy and contact register. Confirm roles with the responsible people. An internal discussion exercise can walk through a clearly fictional event and expose unclear decisions or missing information. Record the plan version, contact verification, exercise notes and assigned corrections. Keep this recommended exercise separate from an actual incident or filing. Check the revised plan again before closing a finding.

Retain evidence that another person can follow

Give each record an identifier and retain its owner, version, date and relevant system or location. Describe observations precisely and record any condition not examined. Keep detailed network information and security weaknesses in the approved evidence store. The working register needs the reference and result, not a copied password or an uncontrolled plant diagram.

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

Give the Board a Decision It Can Act On

Commissioners and governing officials need to understand the effect on service, the work that has been verified and the decisions still required. A technical finding list should lead to a clear account of the unresolved duties, accountable people and resources needed.

Ask what the evidence supports

The brief should state the applicable duty, the scope examined, the evidence supported result and important limitations. Separate facts, professional judgments and unresolved questions. Keep sensitive configurations and detailed weaknesses in a controlled appendix.

Identify the decision and its authority

For each decision, show the service or operating consequence, requested action, accountable official, resources or operating approval needed, deadline and its basis. The technical report's preparer does not automatically become the official authorized to sign a regulatory filing.

Retain the decision and follow the correction

Record the board or delegated official's decision, its date and any conditions. Name the person who will verify the corrective work and identify the record that will demonstrate completion. A progress update should distinguish work performed from work independently checked within the stated scope.

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

Follow the Audit Path

1. Establish applicability

Record the system facts, cited rule, decision, unresolved questions and responsible reviewer.

2. Gather evidence

Retain the record owner, document or observation reference, version, date and relevant population.

3. Examine the control

State the criterion, safe procedure, selected scope, actual observation and limitations.

4. Document the result

Explain the supported result, missing evidence or gap and its significance. An evidence reference must lead to a specific record.

5. Approve corrective work

Record the approved action, accountable owner, deadline, resources and operating constraints.

6. Verify the correction

Check what changed, retain the resulting evidence and state any remaining scope limits before closing the finding.

7. Brief leadership

Present the decisions needed, responsible authority and retained decision record.

8. Maintain the duty

Assign the recurring date or change trigger, record owner and next review. Revisit affected work when the authority or facility changes.

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

EX-DW-01. Fictional drinking water example: an unexplained CVA omission

Fictional training example. This is not a GDF client or a real facility record.

System

Maple Reach is an invented community water system with a recorded population of 12,000. The facility, evidence references and results are fictional teaching material, not GDF client work or an agency submission.

Scope decision

The manager is performing an early readiness review of the cybersecurity vulnerability analysis, or CVA, before the January 1, 2027 compliance date. The examination checks whether its scope accounts for the nine operational locations in the fictional current inventory. It does not test live equipment or determine the effectiveness of every technical control.

Requirement

NY-DW-CVA-REVIEW identifies the annual review and qualifying infrastructure change duties. NY-DW-CVA-CONTROLS identifies the coverage criterion. The fictional applicability record cites those entries and the recorded system facts. A real system must retain its own facts, coverage decision and reviewer.

Evidence

DW-E01 is the current asset inventory. DW-E02 is the CVA report. DW-E03 is the annual review record. DW-E04 contains original notes for the ninth location and DW-E05 is the dated location cross reference. The completed example log below identifies the fictional versions, owners and review dates. It demonstrates an evidence index; the described source documents are not real facility records or separate downloads.

Examination

The reviewer compared the CVA scope with all nine locations in DW-E01. Eight locations could be traced to the analysis. The ninth appeared in a diagram but lacked a clear scope record. No network connection or production test was performed.

Finding

DW-F01. Evidence is insufficient to establish complete CVA coverage. The annual review cannot explain how one location was included or excluded. This is an evidence and scope question; it is not a conclusion that the site is secure or that a technical vulnerability has been confirmed.

Corrective action

The CVA owner locates the underlying scope notes and adds a dated location cross reference. If the location had not been analyzed, the owner would have to arrange the missing work through an authorized scope. The manager keeps this finding open while the question is unresolved.

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

Retest and verification

The revised evidence contains original notes for the ninth location. The reviewer traces all nine locations to the CVA record and records the versions examined. The scope documentation gap is resolved for the review record examined. No conclusion is drawn about technical controls that were not tested.

Manager approval and leadership record

The manager approves the completed scope cross reference and retains it with the review. A fictional leadership receipt records the limits of the conclusion. No operating change, budget authorization or governing board certification is requested in this example. Responsibility for the next review and qualifying infrastructure changes is assigned.

What remains open

Technical control effectiveness remains outside this documentation examination. Retain the annual and infrastructure change review triggers from NY-DW-CVA-REVIEW. If a real examination identifies a vulnerability or incident, evaluate the separate reporting duties rather than using this example to decide them.

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

EX-WW-01. Fictional wastewater example: an unverified response contact

Fictional training example. This is not a GDF client or a real facility record.

System

Mill Creek is an invented municipal wastewater facility with a SPDES permit and a publicly owned treatment works. The records and results are fictional teaching material. No incident occurred and no agency report was sent.

Scope decision

The manager is preparing the cybersecurity incident response plan. An internal discussion exercise checks whether participants can find the responsible contacts and current plan. The exercise is a recommended usability method, not a claim that the cited provision requires an annual drill.

Requirement

NY-WW-IRP identifies the response plan duty. NY-WW-ERP-CONTACT identifies the contact update duty. NY-WW-NOTIFY-ORAL and NY-WW-NOTIFY-WRITTEN remain separate reporting records with their own triggers, clocks and recipients.

Evidence

WW-E01 is the approved plan version. WW-E02 is its contact register. WW-E03 is the internal exercise record, labeled EXERCISE ONLY throughout. The completed example log below records fictional versions, participants, dates, decisions and retest results. It demonstrates an evidence index; the described source documents are not real facility records or separate downloads.

Examination

Participants walked through an internal contact scenario and separately practiced the reporting clocks for an expressly assumed qualifying cybersecurity incident. They found an alternate contact whose current responsibility had not been confirmed. The contact documentation gap alone was not treated as a reportable incident. No external report was submitted and no live plant action was taken.

Finding

WW-F01. The plan exists, but the records do not establish that the alternate contact is current. Usability is unresolved for that escalation step. The manager must determine whether an actual contact or title change also triggers a required plan update.

Corrective action

The plan owner verifies the current contact and role, records that no actual contact or title change occurred, updates the verification annotation in the controlled register and confirms access to the current copy. This record does not start a legal contact change clock. Any real change must be evaluated under NY-WW-ERP-CONTACT rather than assigned a convenient project date.

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

Retest and verification

A second internal walkthrough uses the revised register. Participants identify the responsible people and locate the current reporting card without the superseded copy. The reviewer records that delivery to an outside recipient was not tested. The contact and controlled copy issue is resolved for the internal pathway examined.

Manager approval and leadership record

The manager approves the verified contact register, removes the superseded working copy and assigns the next contact check. A fictional leadership receipt records the exercise scope and the fact that outside delivery remains untested. No annual compliance certification or agency filing is represented by this internal approval.

What remains open

External communications delivery and other plan functions remain outside this exercise. The completed log supplies the fictional awareness time, qualifying incident premise, responsible internal lead and separate reporting clocks. Both submission and receipt entries say Not submitted. Exercise only. The next recommended exercise date is a management choice, separate from a legal duty or contact change trigger.

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

Completed Fictional Records

Every entry in this log is invented for training. No incident was reported and no outside filing was made.

EX-DW-01

Fictional status: FICTIONAL TRAINING RECORD. Maple Reach, every person, date, document and result below are invented. This is not GDF client work, a facility attestation or an agency submission.

System and applicability record: DW-S01, version 1, November 16, 2026. Invented community water system; 12,000 retail residents and no wholesale population; nine locations L01 through L09. The exercise assumes connected OT and IT, so no connection based exclusion is claimed. The greater than 50,000 combined population duties are outside this stated example.

Owner, reviewer and authority: Casey Reed, fictional water manager and authorized representative, owns the review. Jordan Lane, fictional OT coordinator, owns the CVA evidence. Alex Morgan, fictional internal reviewer, checks the evidence independently of its preparation. These are assigned example roles, not invented professional credentials.

Criterion and review dates: NY-DW-CVA-REVIEW, Appendix 5-E.1(c)(1) and 5-E.5(f), with the coverage criterion in NY-DW-CVA-CONTROLS, 5-E.5(d). Prior fictional review: November 20, 2025. This early readiness review opened November 16, 2026 and its scope documentation check closed November 18, 2026. January 1, 2027 is the initial compliance date, not a new deadline created by this example.

DW-E01 and DW-E02 evidence: DW-E01: Location and asset inventory, version 3, approved November 13, 2026; locations L01 through L09. DW-E02: Cybersecurity vulnerability analysis, version 2, dated November 19, 2025. Jordan Lane is the fictional custodian for both records.

DW-E03, DW-E04 and DW-E05 evidence: DW-E03: Annual CVA review record, version 1, opened November 16, 2026 and closed for this documentation check November 18, 2026. DW-E04: Original L09 analysis notes dated November 18, 2025, located November 17, 2026. DW-E05: Location cross reference, version 1, dated November 17, 2026. Example index location: training/EX-DW-01/. These are fictional record references, not supplied evidence files.

Authorized examination and initial result: Alex Morgan compared all nine inventory locations to DW-E02 on November 16, 2026. Eight were traceable; L09 had no clear cross reference in the reviewed version. Examination was limited to document comparison. No equipment access, scanning or operational change was authorized or performed.

Finding DW-F01: Opened November 16, 2026. Evidence is insufficient to establish how L09 was included in the CVA. Status: open pending the original notes or appropriately scoped additional analysis. This is a documentation finding, not confirmation of a technical vulnerability or a safe system.

Corrective action DW-A01: Jordan Lane located DW-E04 and prepared DW-E05 on November 17, 2026. Casey Reed assigned November 18, 2026 as the internal completion target. That target is a management date, not a regulatory correction deadline. No plant equipment was changed.

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

Retest and acceptance record DW-V01: Alex Morgan retested on November 18, 2026 using DW-E01 version 3, DW-E02 version 2, DW-E04 and DW-E05 version 1. All nine locations could be traced to the original CVA evidence. Acceptance: the L09 scope documentation omission is resolved. Result is limited to document traceability; technical control effectiveness was not tested.

Approval and leadership receipt DW-D01: Casey Reed approved closure of DW-F01 at 14:00 EST on November 18, 2026. Avery Quinn, fictional water commissioner, acknowledged the scoped leadership brief at 15:00 EST. The receipt records no budget request, no operating authorization and no broader compliance certification. This example does not create a governing board approval duty for this population band.

Remaining work and next review: Jordan Lane owns any technical control work outside this document check. Casey Reed scheduled the next annual review for November 1, 2027 as an internal target and must separately track the rule requiring review within 30 days after a qualifying major water facility infrastructure change becomes operational. No qualifying change is asserted in this example.

Reporting decision and limitation: This documentation omission alone establishes neither a qualifying vulnerability nor a qualifying cybersecurity incident. No agency report is represented. A real discovery requires a separate decision under NY-DW-VULN-NOTICE and NY-DW-INCIDENT-NOTICE using the actual facts and trigger times.

EX-WW-01

Fictional status: FICTIONAL TRAINING RECORD. Mill Creek, every person, date, document, event premise and result below are invented. EXERCISE ONLY. No actual incident, external notification, annual certification or plant change occurred.

System and applicability record: WW-S01, version 1, November 17, 2026. Invented municipal SPDES permittee and POTW with a design flow of 4 MGD. This example covers early plan readiness and an incident reporting clock exercise. It does not claim compliance with all POTW duties; the 10 MGD logging threshold is not met on these stated facts.

Owner, reviewer and participants: Taylor Bennett, fictional plant manager, owns the plan and is the internal reporting lead for the exercise. Morgan Lee, fictional operator, and Jamie Chen, fictional IT coordinator, participate. Robin Ellis, fictional internal reviewer, records the observations and retest. These role assignments do not confer statutory signing authority for an annual compliance certification.

Criterion and exercise date: NY-WW-IRP and NY-WW-ERP-CONTACT identify the plan and contact duties. NY-WW-EXERCISE is recommended practice, not a mandatory annual drill. NY-WW-NOTIFY-ORAL and NY-WW-NOTIFY-WRITTEN govern the separate qualifying incident exercise. Internal session: November 18, 2026, 08:45 to 10:45 EST.

WW-E01 and WW-E02 evidence: WW-E01: Emergency response plan including its cybersecurity incident response plan, version 1, approved by Taylor Bennett November 17, 2026. WW-E02: Controlled contact register, version 1, dated November 17, 2026; revised verification annotation in version 2, November 18, 2026. Example index location: training/EX-WW-01/. These are fictional record references, not supplied evidence files.

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

WW-E03 exercise record: WW-E03: EXERCISE ONLY contact and reporting walkthrough, version 1, November 18, 2026. Participants used WW-E01 version 1 and WW-E02 version 1. No external calls, agency forms, delivery tests, network scans or live equipment actions were performed.

Finding WW-F01: At 09:20 EST, Robin Ellis recorded that the alternate contact in WW-E02 lacked a dated role confirmation. The records did not establish current responsibility. The finding is a contact documentation gap; it is not itself an assumed or actual reportable cybersecurity incident.

Corrective action WW-A01 and trigger decision: Jamie Chen confirmed the same alternate contact and role with the fictional responsible office at 10:00 EST and annotated WW-E02 version 2. No actual change of contact or title was identified, so this finding does not start a 30 day contact change clock. Taylor Bennett set 10:30 EST as the internal target, not a legal deadline.

Retest and acceptance record WW-V01: At 10:30 EST on November 18, 2026, Robin Ellis repeated the internal walkthrough with Morgan Lee using WW-E01 version 1 and WW-E02 version 2. The current primary and alternate roles and reporting card were found without the superseded copy. Acceptance is limited to this internal pathway. Outside availability and delivery were not tested.

Approval and leadership receipt WW-D01: Taylor Bennett approved closure of WW-F01 at 10:45 EST on November 18, 2026. Drew Parker, fictional municipal administrator, acknowledged the scoped brief at 11:30 EST. The superseded contact working copy was marked obsolete; its history was retained. The receipt is neither an annual certification nor an agency filing.

Separate clock exercise premise: EXERCISE ONLY. For clock practice, assume a cybersecurity incident prevents timely reporting required by the SPDES permit, satisfying the qualifying incident premise in 750-1.2(a)(27). This assumed event is separate from WW-F01. The fictional permittee becomes aware at November 18, 2026, 09:00 EST.

Oral notice clock and recipient: EXERCISE ONLY. Under 750-2.7(h), notify the DEC regional water engineer as soon as possible, with November 19, 2026, 09:00 EST as the 24 hour outer limit from the assumed awareness time. Do not wait for that limit. Current DEC implementation guidance directs the initial online form followed immediately by oral notice to the regional water engineer or manager, with DEC Dispatch as the unreachable contact fallback.

Oral notice submission: Not submitted. Exercise only. Taylor Bennett is the fictional internal lead; no real reporting channel was used.

Oral notice receipt: Not submitted. Exercise only. There is no agency acknowledgement or delivery confirmation.

Written report clock and recipient: EXERCISE ONLY. Under 750-2.7(h), the 30 day written report outer limit is December 18, 2026, 09:00 EST, calculated from the same November 18 awareness time. The clock does not start at the oral notice. Current DEC implementation guidance uses its online follow up form. Retain all required report contents and the actual receipt for any real report.

Written report submission: Not submitted. Exercise only. No written incident report was filed.

Written report receipt: Not submitted. Exercise only. There is no agency acknowledgement or delivery confirmation.

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

Remaining work and next exercise: Taylor Bennett scheduled an internal contact check for February 18, 2027 and a further discussion exercise for November 18, 2027 as management choices. Neither date is an agency drill deadline. External delivery, full plan performance, other reporting duties and annual certification authority remain outside this completed exercise.

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

Working Terms

Applicability

The documented decision about whether a duty covers the system and circumstances, based on facts and the cited authority.

Binding requirement

A duty established by an applicable law, regulation, permit or other binding authority. Its scope and conditions matter.

Incorporated reference

A document or specified provisions made applicable by another authority. Use the edition and scope that authority identifies.

Guidance or recommended practice

Material that explains implementation or supports sound assessment work. Record its status instead of presenting every recommendation as a legal duty.

Criterion

The specific requirement against which evidence is examined. A test and its acceptance criterion must address the same regulatory track.

Evidence reference

An identifier that leads to a retained document, configuration record or observation, with enough version and scope information for another reviewer to find it.

CVA

Cybersecurity vulnerability analysis, the term used in New York DOH Appendix 5-E. Consult that rule for its required scope, timing and follow up. Other programs may use the word assessment for a different document.

ERP and IRP

Emergency response plan and incident response plan. Preserve the plan names, required contents and relationships used by the applicable program.

POTW

Publicly owned treatment works. Establish the facility's actual status from its records before applying duties that depend on that status.

SPDES

State Pollutant Discharge Elimination System, New York's discharge permit program. The actual permit and applicable rules belong in the scope review.

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

DOH and DEC

New York State Department of Health and New York State Department of Environmental Conservation. Their water programs have separate duties and reporting paths.

OT and SCADA

Operational technology and supervisory control and data acquisition. These terms describe systems used to monitor or control physical processes; establish which systems the actual assessment covers.

Verified for the stated scope

A result supported by the examination and evidence recorded. It does not extend to an unexamined system, condition or legal question.

Get Help With the Gaps

GDF can help scope the assessment, agree safe evidence methods and turn findings into work your team can act on. The initial consultation is free. Call (800) 868-8189. Keep sensitive plant records out of the contact form.

https://evestigate.com/resources/ny-water-cybersecurity-toolkit/

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