Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/ot-backup-recovery-checklist/

STANDARDS PREPARATION CHECKLIST

Could You Restore Your OT System?

Gather the digital, physical and procedural dependencies needed to restore selected OT functions.

Baseline: NIST SP 1339, final, June 2026. Prepared November 1, 2026.

Use the questions to prepare the review

Plan restore exercises on nonproduction systems with engineering approval. A functional recovery test completes what the backup integrity checks begin.

For this OT recovery plan, sort the answers into those backed by a record you can locate and those still being confirmed. Give every open question an owner and write down the reason for each exclusion.

Controller programs, license secrets and recovery credentials move through a transfer process agreed for recovery material. Arrange a suitable transfer process for recovery material.

Use these selected OT recovery plan questions to prepare a discussion. The references support the topics.

BK-01

Are all important configuration bearing devices included?

Start with the devices supporting the process as well as the servers. Controllers, drives, switches and field equipment can hold settings needed for recovery.

Evidence to gather

Inventory, configuration owners, criticality and known backup coverage.

To complete the record

Reconcile the backup list with the current OT inventory and record each device added.

Topic reference: NIST SP 1339; Prerequisites; PDF page 1.

Answer:

Owner, evidence reference and follow up date:

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

BK-02

Is backup frequency tied to changes and operational need?

A controller change made through an engineering tool is captured by a change linked backup alongside the daily server backup. Choose the capture and retention approach for each asset and its change pattern.

Evidence to gather

Backup schedules, retention rationale and change linked capture process.

To complete the record

Match each approved change to the recoverable backup that reflects it, and schedule a capture for any change still to be included.

Topic reference: NIST SP 1339; Identify backups required for each asset; PDF page 1.

Answer:

Owner, evidence reference and follow up date:

BK-03

Do you have the files needed to rebuild each critical function?

The recovery package may need logic, firmware, HMI graphics, I/O lists, operating system images and network settings. Listing each item by name and version brings every dependency into view.

Evidence to gather

Per asset recovery package list and version/compatibility information.

To complete the record

Ask the responsible engineer to explain the reconstruction steps and the material still to be gathered.

Topic reference: NIST SP 1339; Identify assets critical to operations; PDF page 1.

Answer:

Owner, evidence reference and follow up date:

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

BK-04

Are the engineering tools, licenses and cables available?

A usable backup is opened with the correct utility, license and physical interface. Confirm that recovery staff can obtain them through an alternate route when the normal office or supplier is out of reach.

Evidence to gather

Engineering tool versions, licenses, interfaces, manuals and access arrangements.

To complete the record

Confirm access and compatibility, then mark the backup package complete.

Topic reference: NIST SP 1339; Manage procedures for backup and recovery; PDF page 2.

Answer:

Owner, evidence reference and follow up date:

BK-05

Can you obtain compatible replacement equipment in time?

A spare must work with the retained program and configuration. Recovery objectives should account for hardware availability, supplier delays and the effort to rebuild a device.

Evidence to gather

Compatible spares list, supplier arrangements and recovery time assumptions.

To complete the record

Identify the critical component with the longest replacement time and plan for it first.

Topic reference: NIST SP 1339; Identify assets critical to operations; PDF page 1.

Answer:

Owner, evidence reference and follow up date:

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

BK-06

Are backups protected from the same event as production?

Review storage locations, access and exposure to modification or destruction. Replication supports continuity, and an independent copy holds a known good version if an unwanted change is replicated. Select protection appropriate to the recovery purpose.

Evidence to gather

Onsite/offsite locations, permissions, storage protection and integrity controls.

To complete the record

Review independent recovery copies and the people able to change or remove them.

Topic reference: NIST SP 1339; Identify backups required for each asset; PDF page 1.

Answer:

Owner, evidence reference and follow up date:

BK-07

Can backup versions be identified and checked before use?

Record the source system, capture time and version. Use suitable integrity checks where supported and retain the engineering basis for accepting a configuration. A matching hash confirms the file is unchanged, and the engineering review checks the logic itself.

Evidence to gather

Labels/index, stored hashes where feasible, trusted versions and engineering verification records.

To complete the record

Trace each backup to its source and version, then rely on it for a restoration.

Topic reference: NIST SP 1339; Identify backups; backup integrity testing and restoration; PDF page 1.

Answer:

Owner, evidence reference and follow up date:

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

BK-08

Are backup procedures part of change management?

Changes to logic, firmware or supporting tools call for a refreshed recovery package. Define when a change triggers a new backup, a compatibility check or an update to restoration instructions.

Evidence to gather

Change records, updated packages and approval history.

To complete the record

Add the recovery tasks to the relevant change process.

Topic reference: NIST SP 1339; Identify backups; manage procedures; PDF page 1.

Answer:

Owner, evidence reference and follow up date:

BK-09

Have restore exercises demonstrated the required function?

Use nonproduction systems to check that retained material can be restored and that the resulting system behaves as intended. Record exceptions and the conditions actually exercised.

Evidence to gather

Exercise date, equipment/version, steps, functional results and open items.

To complete the record

Plan a safe representative exercise, and list each recovery assumption as tested or scheduled for testing.

Topic reference: NIST SP 1339; Backup integrity testing and restoration; PDF page 2.

Answer:

Owner, evidence reference and follow up date:

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

BK-10

Does the chosen hot, warm or cold approach meet the need?

Different approaches trade immediate failover against rebuild effort and cost. Choose the approach per function and account for the resources needed to restore service. The guide leaves the choice of approach to the function each asset serves.

Evidence to gather

Recovery strategy, dependencies, expected recovery time and operating rationale.

To complete the record

Have operations validate the selected approach against the critical function.

Topic reference: NIST SP 1339; Manage procedures for backup and recovery; PDF page 2.

Answer:

Owner, evidence reference and follow up date:

BK-11

Are engineering documents available during an outage?

Network and wiring drawings, control narratives, logic printouts and safety documentation support the work when electronic systems are offline. Identify how staff retrieve usable printed or offline copies.

Evidence to gather

Current document set, printed/offline access and responsible owner.

To complete the record

Complete the document set needed to verify and troubleshoot the planned restoration.

Topic reference: NIST SP 1339; Save engineering documents for a layered approach; PDF page 2.

Answer:

Owner, evidence reference and follow up date:

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

BK-12

Do recovery exercises change the plan?

A useful exercise produces specific corrections alongside the completion record. Feed tool needs, spare compatibility findings and procedural improvements back into backup and change processes.

Evidence to gather

Lessons, assigned actions, updated instructions and follow up evidence.

To complete the record

Assign owners to the open recovery items and review them before the next exercise.

Topic reference: NIST SP 1339; Backup integrity testing and restoration; PDF page 2.

Answer:

Owner, evidence reference and follow up date:

Web Addresses for the Sources Cited

1. NIST SP 1339; Prerequisites; PDF page 1: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1339.pdf#page=1
2. NIST SP 1339; Manage procedures for backup and recovery; PDF page 2: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1339.pdf#page=2

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 1, 2026.

Start With a Free Consultation

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

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

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