STANDARDS PREPARATION CHECKLIST

Prove You Can Restore Your OT System

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

Edition 2026-11-03 · Updated November 3, 2026 · miami-computer-forensics.com/guides/ot-backup-recovery-checklist/

Baseline: NIST SP 1339, final, June 2026. Updated November 3, 2026.

Use the questions to prepare the review

Plan restore exercises on non production systems with engineering approval. Prove recovery with a functional restore test; an integrity check confirms the backup file, and the restore test confirms the running process.

For this OT recovery plan, distinguish records you can locate from answers awaiting confirmation. Mark an answer verified once someone has checked the record behind it. Assign an owner to unresolved questions and explain exclusions.

Note where controller programs, license secrets and recovery credentials are held, and we arrange a secure transfer process for recovery material on the first call.

Use these OT recovery plan questions to prepare the discussion. Each question cites the NIST section it comes from, so your team can check the source directly.

BK-01

Are all important configuration bearing devices included?

Start with the devices supporting the process, not only servers. Controllers, drives, switches and field equipment can hold settings needed for recovery.

Evidence to gather

Inventory, configuration owners, criticality and known backup coverage.

If something is missing

Reconcile the backup list with the current OT inventory and record omissions.

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 daily server backup may not capture a controller change made through an engineering tool. 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.

If something is missing

Identify which approved changes are reflected in a recoverable backup and which are pending.

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. Recording only a file count can conceal a missing dependency.

Evidence to gather

Per asset recovery package list and version/compatibility information.

If something is missing

Ask the responsible engineer to explain the reconstruction steps and missing material.

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?

Restoring a backup takes the correct utility, license and physical interface. Confirm that recovery staff can obtain them when the normal office or supplier is unavailable.

Evidence to gather

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

If something is missing

Resolve access and compatibility before calling a 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?

Confirm that each spare works 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.

If something is missing

Identify the critical component whose replacement time most threatens recovery.

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 can support continuity but may also copy an unwanted change. Select protection appropriate to the recovery purpose.

Evidence to gather

On site/off site locations, permissions, storage protection and integrity controls.

If something is missing

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 proves the file is unchanged, and an engineer confirms the logic is the correct version.

Evidence to gather

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

If something is missing

Resolve ambiguous or untraceable backups before relying on them 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 can invalidate an older 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.

If something is missing

Add the missing 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 non production 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 unresolved gaps.

If something is missing

Plan a safe representative exercise. Keep untested recovery assumptions explicitly open.

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. NIST presents these as options, so match the approach to each asset.

Evidence to gather

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

If something is missing

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 can be needed when electronic systems are unavailable. Identify how staff can retrieve usable copies.

Evidence to gather

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

If something is missing

Close gaps in the documents 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, not only a completion record. Feed missing tools, incompatible spares and procedural problems back into backup and change processes.

Evidence to gather

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

If something is missing

Assign owners to the unresolved recovery problems 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:

Test Your Recovery Plan With an OT Lead

Bring the critical function you need to recover, the backup material you hold and your operating constraints to a free scoping call with a senior GDF OT security lead. On that first call we agree which systems to examine first, how a restore exercise can run safely and what the review will deliver. Call (786) 219-1210 or the 24/7 hotline at (800) 868-8189, or write to info@evestigate.com. To keep preparing, browse the OT security guide library.

Talk to a Senior GDF Security Lead

Bring this checklist to a free scoping call. We review your answers, confirm the systems and operating limits that matter and set out the testing depth, the timeline and the deliverables.

Miami office: (786) 219-1210 · **24/7 hotline:** (800) 868-8189 · **Email:** info@evestigate.com

miami-computer-forensics.com

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