OT Backup and Recovery Readiness Checklist

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

Edition 2026-11-03 · Online at newyorkcomputerforensics.com/guides/ot-backup-recovery-checklist/

Use the questions to prepare the review

Plan restore exercises on nonproduction systems with engineering approval. A functional restore confirms recovery, alongside the backup integrity checks.

For this OT recovery plan, distinguish records you can locate from answers still to be confirmed. Assign an owner to each open question and explain exclusions.

Arrange a suitable transfer process for controller programs, license secrets and recovery credentials.

BK-01

Are all important configuration bearing devices included?

Start with the devices supporting the process, alongside 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 this item

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:

BK-02

Is backup frequency tied to changes and operational need?

Capture controller changes made through an engineering tool 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 this item

Identify approved changes awaiting a recoverable backup.

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

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

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. Record each dependency alongside the file count.

Evidence to gather

Per asset recovery package list and version/compatibility information.

To complete this item

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:

BK-04

Are the engineering tools, licenses and cables available?

Keep the utility, license and physical interface each backup needs alongside it. 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.

To complete this item

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?

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.

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

To complete this item

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:

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.

To complete this item

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.

Evidence to gather

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

To complete this item

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:

BK-08

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

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.

To complete this item

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 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 gaps.

To complete this item

Plan a safe representative exercise. List each recovery assumption with the exercise that will test it.

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

Answer:

Owner, evidence reference and follow up date:

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.

Evidence to gather

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

To complete this item

Have operations validate the selected approach against the critical function.

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

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

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.

To complete this item

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:

BK-12

Do recovery exercises change the plan?

A useful exercise produces specific corrections. 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.

To complete this item

Assign owners to the open 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:

All five checklists are also in one editable workbook: GDF Standards Readiness Checklists (XLSX).

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

Scope Your Assessment

The first call is a free consultation with a senior security lead. We review the systems, the review or audit you face and its timing, and recommend the assessment depth that answers it. Requests are handled in confidence.

Call (800) 868-8189, 24/7 · New York office (212) 561-5860

Email info@evestigate.com or request your consultation at newyorkcomputerforensics.com/contact.

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