OT Security Assessment Preparation

Prepare the scope, records and decisions for an OT security review. Covers selected program, architecture, access, change and recovery topics.

Edition 2026-11-03 · Online at newyorkcomputerforensics.com/guides/ot-security-assessment-checklist/

Use the questions to prepare the review

Start with document review and existing records. Production scanning, intrusive testing, changes and restore exercises each follow their own authorization, engineering review and safety plan.

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

Keep network credentials and sensitive OT configuration details in controlled records. Share only the evidence references in an introductory worksheet.

OT-01

Which processes and sites are included?

An OT review is set by an operational boundary. Include control systems, supporting engineering tools, remote sites and business connections that can affect the process. List exclusions so the coverage of the review is clear.

Evidence to gather

Site/process list, system boundaries, accountable process owner and known exclusions.

To complete this item

Have operations and engineering agree on the boundary before collecting technical records.

Topic reference: NIST SP 800-82 Rev. 3; Sections 2.2 and 4.1.1; PDF page 63.

Answer:

Owner, evidence reference and follow up date:

OT-02

Who can approve the work and accept the remaining risk?

Identify operational, engineering and security decision makers, including who approves a shutdown, a process change or an exception, and the person who owns each open risk.

Evidence to gather

Program charter, responsibility assignments, approval paths and escalation contacts.

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

To complete this item

Name the decision makers and distinguish access approval from permission to test or change a system.

Topic reference: NIST SP 800-82 Rev. 3; Sections 3.1 and 3.3.1 to 3.3.2; PDF page 55.

Answer:

Owner, evidence reference and follow up date:

OT-03

What could a cyber event do to people, the environment or the process?

List the consequences of incorrect control, loss of visibility and loss of availability. A security measure that looks reasonable for office IT can create an unacceptable operating condition in OT.

Evidence to gather

Existing hazard/risk reviews, critical functions, safety constraints and engineering assumptions.

To complete this item

Discuss the consequences with the process and safety owners before selecting assessment methods.

Topic reference: NIST SP 800-82 Rev. 3; Section 4.1.1, OT specific guidance; PDF page 63.

Answer:

Owner, evidence reference and follow up date:

OT-04

Which assessment methods are safe for this equipment?

Document fragile or unsupported components, prohibited activities, stop conditions and approved windows. Passive observation reduces interactions, and monitoring equipment is installed with operations because it can interrupt a connection.

Evidence to gather

Approved scope, vendor constraints, test restrictions, stop authority and offline test options.

To complete this item

Begin with records and interviews. Obtain an approved method before using tools on production equipment.

Topic reference: NIST SP 800-82 Rev. 3; Section 4.3.5, Table 10; section 6.3.2.4; PDF page 80.

Answer:

Owner, evidence reference and follow up date:

OT-05

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

Can you identify the OT assets and their owners?

Include controllers, HMIs, engineering workstations, network devices and supporting servers. Record model, software/firmware version, location and responsibility where available. Add isolated and non IP equipment from engineering records to the discovery result.

Evidence to gather

Current inventory, source/date of each record, owners and an identified unknown assets list.

To complete this item

Reconcile existing engineering records with approved observation and manual checks before adding automated discovery.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.1.1 and 6.1.1.2; PDF page 108.

Answer:

Owner, evidence reference and follow up date:

OT-06

Which assets matter most to continuing safe operations?

Two similar devices may have very different consequences if unavailable or manipulated. Identify process dependence and recovery order so limited assessment time is directed to important functions.

Evidence to gather

Criticality rationale, process dependencies, single points of failure and recovery priorities.

To complete this item

Ask operations to explain the impact of losing each critical function rather than ranking by device count.

Topic reference: NIST SP 800-82 Rev. 3; Sections 4.1.1 to 4.1.2 and 5.3.2; PDF page 63.

Answer:

Owner, evidence reference and follow up date:

OT-07

Do the diagrams show the connections that actually exist?

Include IT/OT boundaries, vendor paths, remote stations, wireless links and cloud services. Record who last checked each diagram against the environment.

Evidence to gather

Dated network diagrams, connection inventory, remote access paths and known undocumented links.

To complete this item

Resolve the important discrepancies with engineering. Confirm current isolation against the live environment.

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

Topic reference: NIST SP 800-82 Rev. 3; Section 6.1.1.2; PDF page 109.

Answer:

Owner, evidence reference and follow up date:

OT-08

Are required communications documented?

Identify source, destination, direction, protocol and operational purpose for important traffic. This gives the team a basis for assessing rules and abnormal behavior without treating every observed connection as necessary.

Evidence to gather

Approved data flow list, process purpose, owners and available observations.

To complete this item

Have system owners explain unknown or undocumented flows before proposing restrictions.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.1.1.1; PDF page 109.

Answer:

Owner, evidence reference and follow up date:

OT-09

Are network segments separated by effective controls?

Review enforcement between business networks, OT zones and management paths against required communications and safety needs, so the rules themselves show which traffic is permitted.

Evidence to gather

Architecture, firewall/ACL exports, allowed flows and the latest approved rule review.

To complete this item

Arrange a configuration review first. Any live validation needs an agreed operational method.

Topic reference: NIST SP 800-82 Rev. 3; Section 5.2.3.1; PDF page 88.

Answer:

Owner, evidence reference and follow up date:

OT-10

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

Can management connections bypass the intended boundary?

Check for second network interfaces, temporary connections, remote tools and maintenance paths that bridge segments. Evaluate their purpose and controls instead of applying an unexplained blanket ban on a hardware feature.

Evidence to gather

Management path inventory, interfaces, remote tools and approved exceptions.

To complete this item

Have engineering review each bridge and document how the intended boundary is maintained.

Topic reference: NIST SP 800-82 Rev. 3; Section 5.2.3.1; section 6.2.5; PDF page 88.

Answer:

Owner, evidence reference and follow up date:

OT-11

How are physical access and remote locations controlled?

Cabinets, control rooms and field equipment can be reached through physical routes as well as network paths. Identify who can enter, how visitors are handled and whether unstaffed sites have suitable protection.

Evidence to gather

Access lists, visitor process, cabinet controls, site checks and responsible owners.

To complete this item

Review the highest consequence locations with the physical security and operations teams.

Topic reference: NIST SP 800-82 Rev. 3; Section 5.2.2; PDF page 86.

Answer:

Owner, evidence reference and follow up date:

OT-12

Do access permissions follow current responsibilities?

Identify operator, engineer, administrator and vendor permissions. Include how accounts are issued, changed and removed. Give shared or legacy access a documented reason and compensating measures.

Evidence to gather

Account/role list, approval records, departures/role changes and exceptions.

To complete this item

Reconcile accounts with current authorized personnel and escalate unexplained privileged access.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.2.1 and 6.2.1.1; PDF page 114.

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

Answer:

Owner, evidence reference and follow up date:

OT-13

Can operators still act safely during an authentication failure?

Set authentication and session lock to fit urgent operator action. Identify where technical limitations or emergency needs change the design and how access remains controlled in those cases.

Evidence to gather

Emergency access procedure, HMI constraints, access safeguards and review approvals.

To complete this item

Review proposed authentication changes with the process and safety owners before applying them.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.2.1, OT specific guidance; PDF page 114.

Answer:

Owner, evidence reference and follow up date:

OT-14

Are vendor connections approved, limited and removed when finished?

Record the business reason, user, permitted systems, access window and removal method. Operations should know when remote work is planned. Place continuous support under a defined arrangement.

Evidence to gather

Vendor access register, approvals, session records and expiry/revocation process.

To complete this item

Review active access with the responsible vendor and operator before scheduling changes.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.2.10; PDF page 139.

Answer:

Owner, evidence reference and follow up date:

OT-15

Where is remote user authentication enforced?

Confirm how remote users are identified and where MFA or compensating controls are applied. Protecting an access gateway is different from adding authentication directly to every controller.

Evidence to gather

Remote access design, identity settings, MFA coverage and documented limitations.

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

To complete this item

Agree on a feasible architecture for unsupported devices instead of forcing an untested change on them.

Topic reference: NIST SP 800-82 Rev. 3; Sections 6.2.1.4.4 and 6.2.10; PDF page 123.

Answer:

Owner, evidence reference and follow up date:

OT-16

Are wireless and cellular connections part of the scope?

Radio and cellular paths can provide access outside the expected wired perimeter. Record ownership, purpose, authentication and the operational effects of losing the link.

Evidence to gather

Wireless/cellular inventory, configurations, providers and engineering requirements.

To complete this item

Identify unknown links and have engineering assess them before changing radio or network settings.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.2.9; PDF page 137.

Answer:

Owner, evidence reference and follow up date:

OT-17

Are control system changes recorded and approved?

A current configuration is most useful when the team can explain who changed it and restore the prior state. Include logic, setpoints where relevant, firmware, network rules and supporting applications in the change process.

Evidence to gather

Approved changes, baseline versions, backup points, test records and rollback instructions.

To complete this item

Reconcile recent changes with the configuration owner and record missing approvals or recovery material.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.2.4.2; PDF page 128.

Answer:

Owner, evidence reference and follow up date:

OT-18

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

How are relevant vulnerabilities identified safely?

Use the asset/version inventory, vendor notices and approved assessment methods to identify exposure. Records and passive methods identify weaknesses alongside scanning, and each method is chosen with care because some tools affect control system communications.

Evidence to gather

Inventory/version records, vendor advisories, review process and approved tool methods.

To complete this item

Start with the known estate and advisories. Assess tool compatibility offline before production use.

Topic reference: NIST SP 800-82 Rev. 3; Sections 6.2.11 and 6.3.2.4; PDF page 141.

Answer:

Owner, evidence reference and follow up date:

OT-19

Are patch decisions based on operational and security risk?

Record applicability, vendor advice, testing, deployment windows and rollback. Where a patch is delayed or unavailable, capture the reason, interim protection and date for reconsideration.

Evidence to gather

Patch decisions, offline test results, exception owner and planned maintenance window.

To complete this item

Ask knowledgeable OT personnel to decide the treatment and set the OT patch schedule.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.2.11; PDF page 141.

Answer:

Owner, evidence reference and follow up date:

OT-20

Are unsupported components managed as a continuing risk?

Old equipment may remain necessary for the process. Identify support status, exposure, spare availability and feasible protective measures. An upgrade plan accounts for engineering dependencies along with the software version.

Evidence to gather

Support/lifecycle register, compensating controls, replacement plan and approved risk decisions.

To complete this item

Assign an owner to each important unsupported component and define the next review milestone.

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

Topic reference: NIST SP 800-82 Rev. 3; Section 5.1.1 and section 6.2.11; PDF page 84.

Answer:

Owner, evidence reference and follow up date:

OT-21

Are maintenance tools and vendor laptops controlled?

Service equipment and software can carry changes or malicious content into the OT environment. Record which tools are approved, how their origin is checked and how maintenance activities are logged.

Evidence to gather

Approved tools, vendor software provenance, maintenance authorizations and activity records.

To complete this item

Review the maintenance entry process with the equipment owner before the next service visit.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.2.5; PDF page 134.

Answer:

Owner, evidence reference and follow up date:

OT-22

Are removable media and portable equipment handled consistently?

Identify how USB devices, portable drives and other media enter, move through and leave the environment. Include authorization, labeling, storage and the treatment of sensitive configuration files.

Evidence to gather

Media procedure, permitted devices, transfer records and storage/sanitization arrangements.

To complete this item

Establish an approved transfer route that engineers can use day to day.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.2.7; PDF page 136.

Answer:

Owner, evidence reference and follow up date:

OT-23

Is malware protection compatible with the control applications?

Security software and signature updates can affect performance or essential files. Identify supported protection, exclusions, update arrangements and the measures used on systems that call for agentless protection.

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

Evidence to gather

Vendor compatibility guidance, protection configuration, exceptions and update/test records.

To complete this item

Review changes with engineering and the vendor before enabling new scans or endpoint agents.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.3.2.3; PDF page 148.

Answer:

Owner, evidence reference and follow up date:

OT-24

Do the available logs cover important changes and access?

List the sources actually recording activity, the events retained and the retention period. Confirm capacity, export and collection for each configured log source. Protect the records needed for later analysis.

Evidence to gather

Sample logs, logging configuration, retention/capacity settings and access controls.

To complete this item

Confirm one representative event is retained through the collection path using an approved verification method.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.2.6.1; PDF page 135.

Answer:

Owner, evidence reference and follow up date:

OT-25

Can timestamps be compared across the relevant systems?

Record time sources, time zones and known clock differences. Accurate time supports troubleshooting and event correlation, but changes to time services can also affect control functions and need engineering review.

Evidence to gather

Time configuration, source dependencies, clock checks and known limitations.

To complete this item

Document discrepancies before changing clocks. Have engineering approve any synchronization change.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.2.12; PDF page 142.

Answer:

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

Owner, evidence reference and follow up date:

OT-26

Who receives and acts on an OT security alert?

A monitoring system pays off when the team understands normal behavior and can act on meaningful deviations. Identify escalation, operating context and response arrangements for remote or unstaffed sites.

Evidence to gather

Alert rules, normal activity baselines, duty contacts and representative handling records.

To complete this item

Choose a representative scenario and confirm the response path through an approved tabletop or review.

Topic reference: NIST SP 800-82 Rev. 3; Sections 6.3.1 to 6.3.3; PDF page 144.

Answer:

Owner, evidence reference and follow up date:

OT-27

Is the organization able to recover the important configurations?

Include controller logic, HMI files, network configurations and the tools and licenses needed to use them. A demonstrated working restoration confirms the copy.

Evidence to gather

Backup inventory, versions, engineering dependencies and recent restore evidence.

To complete this item

Use the OT backup checklist to identify missing recovery dependencies before scheduling a safe exercise.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.2.4.3; PDF page 129.

Answer:

Owner, evidence reference and follow up date:

OT-28

Are recovery objectives and startup dependencies agreed?

Define the tolerable outage and data loss for the important functions. Restoration order may depend on power, communications, safety checks and equipment availability rather than simply restoring servers first.

Evidence to gather

Approved RTO/RPO, startup sequence, dependencies and available spares.

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

To complete this item

Have operations validate the recovery sequence and list each assumption awaiting demonstration.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.2.4.5; PDF page 131.

Answer:

Owner, evidence reference and follow up date:

OT-29

Does the incident plan cover safe containment and continuity?

Disconnecting a suspected device may interrupt an essential process or remove operator visibility. The plan should connect security decisions to operational authority, safety conditions and alternatives such as controlled manual operation.

Evidence to gather

Incident plan, decision authority, safe operating limits and emergency contacts.

To complete this item

Walk through a plausible scenario with engineering and operations before relying on a generic IT playbook.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.2.4.5, OT specific guidance; PDF page 133.

Answer:

Owner, evidence reference and follow up date:

OT-30

Have the relevant people practiced their roles?

Operators, maintainers, IT, security and outside providers need to know their part in an incident or recovery. Exercises show the plan working under pressure.

Evidence to gather

Role specific training, exercise records, lessons and outstanding actions.

To complete this item

Plan an authorized tabletop that includes the important operational decisions and external dependencies.

Topic reference: NIST SP 800-82 Rev. 3; Sections 3.3.5 and 6.2.4.5; PDF page 58.

Answer:

Owner, evidence reference and follow up date:

OT-31

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

Are power and environmental dependencies included?

Cooling, reliable power and environmental protection support the control equipment. Record what happens during a power interruption, how equipment reaches a safe state and who maintains the supporting protection.

Evidence to gather

Power/UPS arrangements, environmental monitoring and maintenance records.

To complete this item

Review critical dependencies with facilities and engineering without changing live power or safety systems.

Topic reference: NIST SP 800-82 Rev. 3; Section 6.2.4.4; PDF page 130.

Answer:

Owner, evidence reference and follow up date:

OT-32

Are significant exceptions assigned and revisited?

Where a recommended protection does not fit a particular device, record the reason, the accepted risk, interim measures and the decision owner. Keep each exception visible after the assessment is filed.

Evidence to gather

Risk/exception register, approvals, treatment actions and review dates.

To complete this item

Agree on a risk based action plan and who can accept residual exposure.

Topic reference: NIST SP 800-82 Rev. 3; Sections 3.3 and 4.3.5; PDF page 54.

Answer:

Owner, evidence reference and follow up date:

Final guidance and draft updates

SP 800-82 Rev. 3 is the final baseline used here. Rev. 4, dated September 21, 2026, is an initial public draft and is read here as guidance in progress. The July 2024 potential update corrects a control identifier in Appendix F and leaves these selected questions as they are.

NIST final publication record and potential updates | Revision 4 draft record

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.