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

STANDARDS PREPARATION CHECKLIST

OT Security Assessment Preparation

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

Baseline: NIST SP 800-82 Rev. 3, final. Prepared November 1, 2026.

Use the questions to prepare the review

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

For this OT security review, separate the records you can locate from the answers your team is still confirming. Give each open question an owner and record the reason for each exclusion.

Share evidence references in the introductory worksheet, and keep network credentials and sensitive OT configuration details in your controlled records.

Use these selected OT security review questions to prepare a discussion. The references support the topics.

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

OT-01

Which processes and sites are included?

An OT review needs an operational boundary, not just an IP range. Include control systems, supporting engineering tools, remote sites and business connections that can affect the process. Identify exclusions so everyone reads a focused review for the scope it covers.

Evidence to gather

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

To complete the record

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?

Authority to approve a shutdown, a process change or an exception often sits above the technical contact. Identify operational, engineering and security decision makers and the person who owns the remaining risk.

Evidence to gather

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

To complete the record

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 3.3.1-3.3.2; PDF page 55.

Answer:

Owner, evidence reference and follow up date:

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

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. Each security measure designed for office IT is weighed against the operating conditions of the process before it is adopted in OT.

Evidence to gather

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

To complete the record

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 sensitive or legacy components, excluded activities, stop conditions and approved windows. Passive observation keeps interaction with the process low, and the installation of monitoring equipment is scheduled and approved like any other work on a live connection.

Evidence to gather

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

To complete the record

Begin with records and interviews, then bring tools to production equipment under an approved method.

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:

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

OT-05

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. Engineering records and manual checks cover isolated or non-IP equipment alongside any discovery result.

Evidence to gather

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

To complete the record

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 assessment time is directed to the most important functions.

Evidence to gather

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

To complete the record

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 4.1.1-4.1.2 and 5.3.2; PDF page 63.

Answer:

Owner, evidence reference and follow up date:

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

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 the date and coverage of each diagram and who last checked it against the environment.

Evidence to gather

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

To complete the record

Resolve the important discrepancies with engineering. Confirm current isolation against current traffic and configuration, using an older drawing as the starting reference.

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, with each observed connection weighed against its documented purpose.

Evidence to gather

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

To complete the record

Have system owners account for each unidentified or undocumented flow, then propose 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:

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

OT-09

Are network segments separated by effective controls?

Firewall and switch configuration shows which traffic is permitted. Review enforcement between business networks, OT zones and management paths against required communications and safety needs.

Evidence to gather

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

To complete the record

Arrange a configuration review first. Live validation then follows 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

Can management connections bypass the intended boundary?

Check for second network interfaces, temporary connections, remote tools and maintenance paths that bridge segments. Evaluate the purpose and controls of each one so the decision rests on how the path is actually used.

Evidence to gather

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

To complete the record

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:

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

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 the record

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. Shared or legacy access carries a documented reason and compensating measures that explain how accountability is maintained.

Evidence to gather

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

To complete the record

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.

Answer:

Owner, evidence reference and follow up date:

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

OT-13

How do operators act safely during an authentication failure?

Authentication and session lock settings are designed around 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 the record

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. Continuous support runs under a defined and documented arrangement.

Evidence to gather

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

To complete the record

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:

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

OT-15

Where is remote user authentication enforced?

Confirm how remote users are identified and where MFA or compensating controls are applied. Authentication can be enforced at an access gateway or directly on a controller, and the record states which applies where.

Evidence to gather

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

To complete the record

Agree on a feasible architecture for legacy devices, protecting them at the gateway and testing any change before it reaches 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 the record

Identify every link, including any not yet documented, and have engineering assess each one, then plan radio or network setting changes.

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

Answer:

Owner, evidence reference and follow up date:

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

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 the record

Reconcile recent changes with the configuration owner and record any approvals or recovery material still to be located.

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

How are relevant vulnerabilities identified safely?

Use the asset/version inventory, vendor notices and approved assessment methods to identify exposure. Weaknesses are identified through the inventory and advisories as well as scanning, and each tool is checked for its effect on control system communications before use.

Evidence to gather

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

To complete the record

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:

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

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 the record

Ask knowledgeable OT personnel to decide the treatment. Set an OT patch schedule around the operating windows rather than the office IT calendar.

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 as well as the software version.

Evidence to gather

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

To complete the record

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

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:

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

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 the record

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 the record

Establish an approved and practical transfer route that engineers will use in their daily work.

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

Answer:

Owner, evidence reference and follow up date:

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

OT-23

Is malware protection compatible with the control applications?

Security software and signature updates are tested against performance and essential files. Identify supported protection, exclusions, update arrangements and the alternative measures used where the device calls for something other than an endpoint agent.

Evidence to gather

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

To complete the record

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 each configured log source end to end, including its capacity, export and collection. Protect the records needed for later analysis.

Evidence to gather

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

To complete the record

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:

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

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, and engineering reviews any change to time services because those services also support control functions.

Evidence to gather

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

To complete the record

Document discrepancies first, then have engineering approve any synchronization change.

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

Answer:

Owner, evidence reference and follow up date:

OT-26

Who receives and acts on an OT security alert?

A monitoring system delivers its value when the team understands normal behavior and acts 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 the record

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

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

Answer:

Owner, evidence reference and follow up date:

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

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 backup, and the file copy is the first step toward it.

Evidence to gather

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

To complete the record

Use the OT backup checklist to identify every recovery dependency, then schedule 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 follows power, communications, safety checks and equipment availability as well as server recovery.

Evidence to gather

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

To complete the record

Have operations validate the recovery sequence and mark each assumption as demonstrated or scheduled for an exercise.

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

Answer:

Owner, evidence reference and follow up date:

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

OT-29

Does the incident plan cover safe containment and continuity?

Containment is planned around the process so operators keep visibility and essential functions keep running. 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 the record

Walk through a plausible scenario with engineering and operations and adapt the IT playbook to the plant.

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 test the plan under realistic pressure and build on the policy acknowledgement.

Evidence to gather

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

To complete the record

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:

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

OT-31

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 the record

Review critical dependencies with facilities and engineering through records and walkdowns, leaving live power and safety systems in their operating state.

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?

Some devices call for an alternative to a recommended protection. Record the reason, the accepted risk, interim measures and the decision owner. An exception should remain visible after the assessment is filed.

Evidence to gather

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

To complete the record

Agree on a risk based action plan and name who accepts the remaining 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:

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

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 tracked here as guidance in development. The July 2024 potential update corrects a control identifier in Appendix F, and these selected questions stand as written.

NIST SP 800-82 Rev. 3 publication record | NIST SP 800-82 Rev. 4 initial public draft

Web Addresses for the Sources Cited

1. NIST SP 800-82 Rev. 3; Sections 2.2 and 4.1.1; PDF page 63: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=63
2. NIST SP 800-82 Rev. 3; Sections 3.1 and 3.3.1-3.3.2; PDF page 55: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=55
3. NIST SP 800-82 Rev. 3; Section 4.3.5, Table 10; section 6.3.2.4; PDF page 80: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=80
4. NIST SP 800-82 Rev. 3; Section 6.1.1 and 6.1.1.2; PDF page 108: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=108
5. NIST SP 800-82 Rev. 3; Section 6.1.1.2; PDF page 109: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=109
6. NIST SP 800-82 Rev. 3; Section 5.2.3.1; PDF page 88: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=88
7. NIST SP 800-82 Rev. 3; Section 5.2.2; PDF page 86: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=86
8. NIST SP 800-82 Rev. 3; Section 6.2.1 and 6.2.1.1; PDF page 114: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=114
9. NIST SP 800-82 Rev. 3; Section 6.2.10; PDF page 139: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=139
10. NIST SP 800-82 Rev. 3; Sections 6.2.1.4.4 and 6.2.10; PDF page 123: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=123
11. NIST SP 800-82 Rev. 3; Section 6.2.9; PDF page 137: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=137
12. NIST SP 800-82 Rev. 3; Section 6.2.4.2; PDF page 128: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=128
13. NIST SP 800-82 Rev. 3; Sections 6.2.11 and 6.3.2.4; PDF page 141: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=141
14. NIST SP 800-82 Rev. 3; Section 5.1.1 and section 6.2.11; PDF page 84: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=84
15. NIST SP 800-82 Rev. 3; Section 6.2.5; PDF page 134: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=134
16. NIST SP 800-82 Rev. 3; Section 6.2.7; PDF page 136: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=136
17. NIST SP 800-82 Rev. 3; Section 6.3.2.3; PDF page 148: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=148
18. NIST SP 800-82 Rev. 3; Section 6.2.6.1; PDF page 135: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=135

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

19. NIST SP 800-82 Rev. 3; Section 6.2.12; PDF page 142: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=142
20. NIST SP 800-82 Rev. 3; Sections 6.3.1-6.3.3; PDF page 144: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=144
21. NIST SP 800-82 Rev. 3; Section 6.2.4.3; PDF page 129: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=129
22. NIST SP 800-82 Rev. 3; Section 6.2.4.5; PDF page 131: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=131
23. NIST SP 800-82 Rev. 3; Section 6.2.4.5, OT specific guidance; PDF page 133: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=133
24. NIST SP 800-82 Rev. 3; Sections 3.3.5 and 6.2.4.5; PDF page 58: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=58
25. NIST SP 800-82 Rev. 3; Section 6.2.4.4; PDF page 130: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=130
26. NIST SP 800-82 Rev. 3; Sections 3.3 and 4.3.5; PDF page 54: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf#page=54
27. NIST SP 800-82 Rev. 3 publication record: https://csrc.nist.gov/pubs/sp/800/82/r3/final
28. NIST SP 800-82 Rev. 4 initial public draft: https://csrc.nist.gov/pubs/sp/800/82/r4/ipd

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 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.