OT Security Audits

Conducting effective security assessments in industrial environments

OT Security Learning Series

Document 730 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Security audits systematically evaluate an organization's security controls against established standards, policies, or regulatory requirements. In OT environments, audits must balance thoroughness with operational safety and often involve unique constraints not found in IT audits.

OT security audit objectives:

- **Compliance verification:** Meet regulatory and industry standards
- **Control assessment:** Evaluate effectiveness of security measures
- **Gap identification:** Find weaknesses before attackers do
- **Risk quantification:** Support risk management decisions
- **Improvement roadmap:** Prioritize security investments

2 Types of OT Security Audits

2.1 Audit Categories

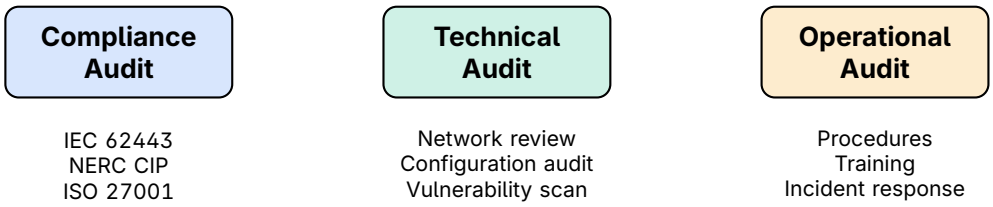

Figure 1: Types of OT Security Audits

2.2 Compliance Audits

Standard	Industry	Focus Areas
IEC 62443	All industrial	Security levels, zones, risk assessment
NERC CIP	Power/utilities	Critical infrastructure protection
NIST 800-82	Government, critical	OT security framework
ISO 27001	General	ISMS with OT scope
TSA Pipeline	Oil & gas pipelines	Cybersecurity directives

Table 1: Common OT Compliance Standards

2.3 Technical Audits

- **Network architecture review:** Segmentation, firewall rules, data flows

- **Configuration audit:** System hardening, default credentials, services
- **Access control review:** User management, privilege levels, authentication
- **Vulnerability assessment:** Known CVEs, missing patches, exposures
- **Backup and recovery:** Configuration backups, restore testing

2.4 Operational Audits

- **Policy and procedure review:** Documentation completeness and currency
- **Training assessment:** Security awareness, role-specific training
- **Change management:** Process effectiveness, documentation
- **Incident response:** Plan review, tabletop exercises
- **Vendor management:** Third-party access controls

3 Audit Planning

3.1 Pre-Audit Activities

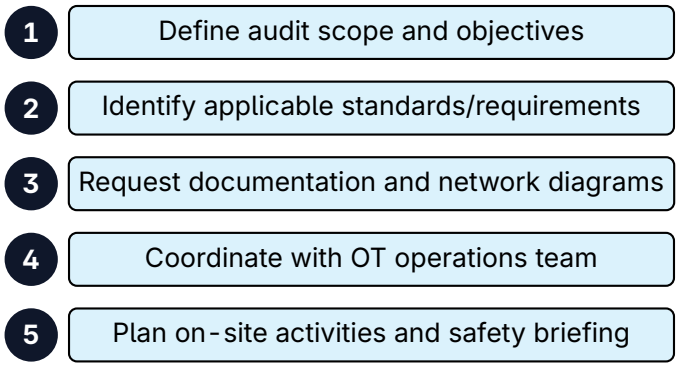

Figure 2: Audit Planning Checklist

3.2 Scope Definition

Element	Considerations
Locations	Which facilities, remote sites?
Systems	All OT assets or specific zones/systems?
Standards	Which frameworks (IEC 62443, NERC CIP, etc.)?
Depth	Full assessment or focused review?
Testing	Passive review only or include active testing?
Timeline	Audit duration, final report deadline

Table 2: Audit Scope Definition Elements

3.3 Stakeholder Engagement

Warning

Critical Stakeholders for OT Audits:

- OT Operations – System access, operational context
- Engineering – Technical documentation, architecture knowledge
- IT Security – IT/OT integration, enterprise policies
- Safety – Safety system considerations, access procedures
- Management – Authorization, resource allocation

4 Audit Execution

4.1 Document Review

Document Type	Review Focus
Network diagrams	Accuracy, segmentation, data flows
Security policies	OT-specific policies, coverage
Procedures	Change management, incident response
Asset inventory	Completeness, currency
Risk assessments	Methodology, findings, treatment
Previous audits	Prior findings, remediation status

Table 3: Documentation Review Areas

4.2 Technical Assessment

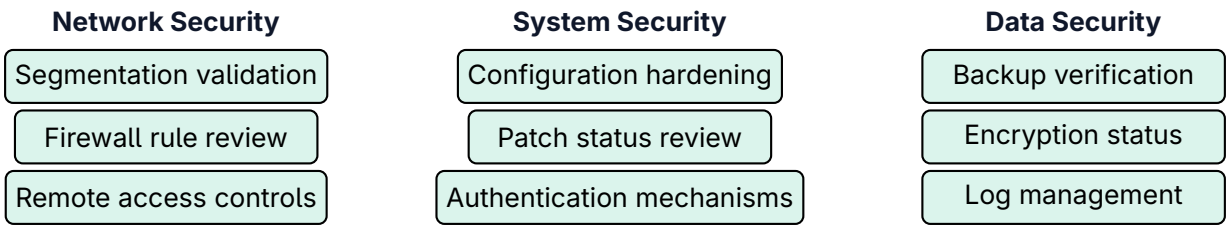

Figure 3: Technical Assessment Areas

4.3 Interview and Observation

- **Operator interviews:** Security awareness, procedure adherence
- **Engineer interviews:** Change management, system knowledge
- **Physical observation:** Access controls, badge usage, unlocked doors
- **Process observation:** How procedures are actually followed

4.4 On-Site Safety Considerations

Critical

Safety Requirements for OT Auditors:

- Complete site safety orientation
- Wear required PPE (hard hat, safety glasses, etc.)
- Never touch or operate OT equipment without authorization
- Coordinate all testing activities with operations
- Know emergency procedures and evacuation routes
- Never compromise safety for audit completeness

5 Common Audit Findings

5.1 Frequently Identified Issues

Finding Category	Common Examples
Network security	Insufficient segmentation, overly permissive rules
Access control	Shared accounts, weak passwords, no MFA
Asset management	Incomplete inventory, unknown devices
Patch management	Outdated systems, no patching process
Remote access	Direct internet connections, no logging
Monitoring	Limited visibility, no alerting
Documentation	Outdated diagrams, missing procedures
Training	No OT security awareness program

Table 4: Common OT Security Audit Findings

5.2 Finding Severity Levels

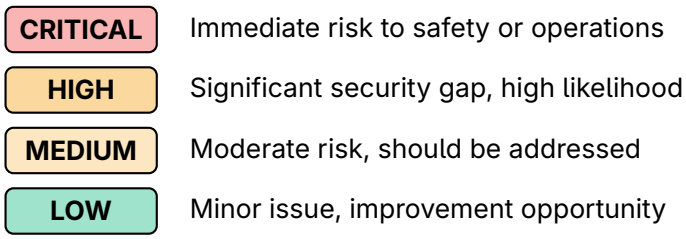

Figure 4: Finding Severity Classification

6 Reporting and Remediation

6.1 Audit Report Structure

Key Point

Effective Audit Report Components:

1. **Executive summary:** Key findings, overall assessment, priorities
2. **Scope and methodology:** What was assessed and how
3. **Detailed findings:** Issue, evidence, risk, recommendation
4. **Prioritized remediation:** Actions ranked by risk and effort
5. **Compliance mapping:** Findings linked to specific requirements
6. **Appendices:** Supporting evidence, technical details

6.2 Finding Documentation

Each finding should include:

- **Description:** Clear explanation of the issue
- **Evidence:** Screenshots, logs, observations
- **Risk:** Potential impact and likelihood
- **Affected systems:** Scope of the issue
- **Recommendation:** Specific remediation guidance
- **Reference:** Related standard/requirement

6.3 Remediation Planning

Figure 5: Finding Remediation Process

7 Audit Program Management

7.1 Audit Frequency

Audit Type	Frequency	Driver
Full compliance audit	Annual	Regulatory requirement
Technical assessment	Semi-annual	Risk management
Focused review	As needed	Major changes, incidents
Self-assessment	Quarterly	Continuous improvement
Third-party audit	1–3 years	Certification, verification

Table 5: Recommended Audit Frequency

7.2 Continuous Improvement

- Track remediation progress against deadlines
- Monitor for recurring findings
- Update audit scope based on threat landscape
- Benchmark against industry peers
- Incorporate lessons from security incidents

7.3 Audit Metrics

- **Findings by severity:** Track distribution over time
- **Remediation rate:** Percentage of findings addressed on time
- **Repeat findings:** Issues that recur between audits
- **Compliance score:** Percentage of requirements met
- **Time to remediate:** Average days from finding to closure

8 Internal vs External Audits

Aspect	Internal Audit	External Audit
Independence	Limited	High
OT knowledge	May be high	Varies by firm
Cost	Lower	Higher
Credibility	Internal use	Third-party verification
Frequency	More frequent	Less frequent
Scope flexibility	High	Often fixed

Table 6: Internal vs External Audit Comparison

Tip

Best Practice: Use internal audits for continuous monitoring and improvement, and external audits for independent verification and certification requirements.

9 Summary

Key Takeaways

- **Multiple audit types:** Compliance, technical, and operational
- **OT-specific considerations:** Safety, availability, operations coordination
- **Thorough planning:** Scope, stakeholders, safety requirements
- **Evidence-based findings:** Document issues with clear evidence
- **Risk-based prioritization:** Focus remediation on highest risks
- **Continuous improvement:** Regular audits drive security maturity
- **Track progress:** Monitor remediation and measure improvement

10 Further Reading

Standards

- **IEC 62443-2-1** – Security management system requirements
  https://webstore.iec.ch/publication/7030
- **IEC 62443-3-2** – Security risk assessment for system design
  https://webstore.iec.ch/publication/30727
- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA** – Assessments and Services
  https://www.cisa.gov/resources-tools/services/cisa-assessments
- **ISACA** – IT Audit Framework
  https://www.isaca.org/

Part of the OT Security Learning Series