OT Tabletop Exercises

Testing Incident Response Through Scenario-Based Discussion

OT Security Learning Series

Document 650 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction **3**

2 Exercise Types **3**
2.1 Tabletop Exercise Characteristics 3

3 Planning and Preparation **3**
3.1 Define Objectives 3
3.2 Develop the Scenario 4
3.3 Prepare Materials 4

4 Key Participants **4**
4.1 Required Roles 5

5 OT-Specific Scenarios **5**
5.1 Scenario Categories 5
5.2 Sample Scenario Structure 5

6 Conducting the Exercise **6**
6.1 Exercise Flow 6
6.2 Facilitation Tips 6
6.3 Key Discussion Questions 6

7 After-Action Review **6**
7.1 Hot Wash 6
7.2 After-Action Report 7

8 Exercise Frequency **7**

9 Summary **8**

10 Further Reading **8**

1 Introduction

Information

Tabletop exercises are discussion-based sessions where participants walk through simulated incident scenarios to test response plans, identify gaps, and improve coordination. For OT environments, these exercises are essential because real-world testing of incident response on production systems is often impossible without risking safety or operations.

Unlike IT environments where systems can often be taken offline for testing, OT systems typically run continuously. Tabletop exercises provide a safe way to validate that teams can respond effectively to cyber incidents affecting industrial processes, without disrupting operations or creating safety hazards.

2 Exercise Types

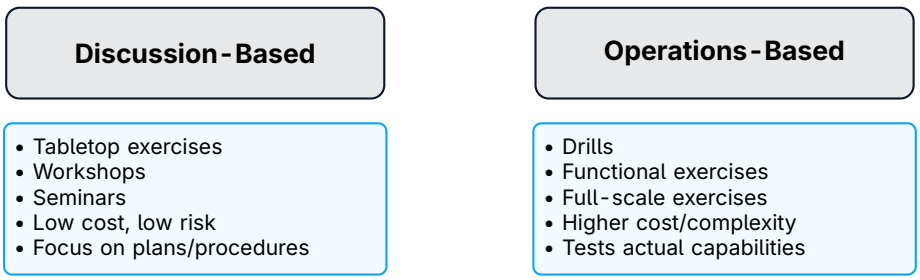

Figure 1: Exercise types by complexity

2.1 Tabletop Exercise Characteristics

- **Format** – Facilitated group discussion around a scenario
- **Duration** – Typically 2–4 hours
- **Resources** – Minimal; requires facilitator and participants
- **Risk** – None to operations; purely discussion-based
- **Output** – Identified gaps, action items, improved awareness

3 Planning and Preparation

3.1 Define Objectives

Before designing an exercise, establish clear goals:

Objective Type	Example
Test procedures	Validate OT incident response plan steps
Identify gaps	Find missing playbooks for specific attack types
Train personnel	Familiarize operators with security escalation
Test communication	Verify notification chains work as documented
Assess decisions	Evaluate criteria for OT system isolation

Table 1: Example exercise objectives

3.2 Develop the Scenario

Effective OT scenarios should be:

- **Realistic** – Based on actual threats to your industry
- **Relevant** – Target systems participants actually manage
- **Challenging** – Force difficult decisions, not obvious answers
- **Scoped** – Achievable within the exercise timeframe

Tip

Base scenarios on real incidents from your sector. Adapt published case studies (Stuxnet, TRITON, Colonial Pipeline) to your specific environment and systems.

3.3 Prepare Materials

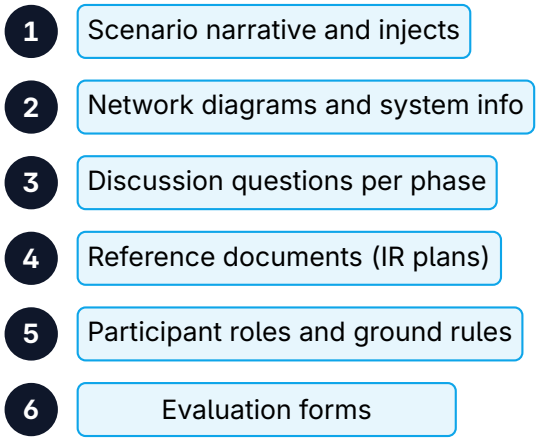

Figure 2: Exercise preparation checklist

4 Key Participants

4.1 Required Roles

Role	Responsibility
Facilitator	Guides discussion, presents injects, keeps time
OT Operations	Represents control room, field operations
OT Engineering	Provides technical system knowledge
IT Security	Brings cybersecurity detection/response expertise
Management	Makes escalation and business decisions
Safety	Ensures safety implications are considered
Communications	Handles internal/external messaging

Table 2: Key exercise participants

Warning

OT tabletop exercises must include operations and engineering staff, not just IT security. Decisions about isolating control systems or shutting down processes require input from those who understand operational consequences.

5 OT-Specific Scenarios

5.1 Scenario Categories

Category	Scenario Examples
Ransomware	Ransomware spreads from IT to historian, threatens HMI
Targeted Attack	APT compromises engineering workstation, modifies PLC logic
Insider Threat	Disgruntled employee with OT access sabotages process
Supply Chain	Vendor's compromised update deployed to RTUs
Safety System	Attacker attempts to disable safety instrumented system
Data Integrity	Process values manipulated to cause unsafe conditions

Table 3: OT-specific scenario categories

5.2 Sample Scenario Structure

A typical tabletop scenario progresses through phases:

1. **Initial Detection** – SOC alerts on suspicious activity
2. **Investigation** – Determine scope, affected systems
3. **Escalation** – IT/OT coordination, management notification
4. **Containment** – Decisions on isolation, operational impact
5. **Eradication** – Remove threat while maintaining operations

6. **Recovery** – Restore systems, verify integrity
7. **Post-Incident** – Lessons learned, improvements

6 Conducting the Exercise

6.1 Exercise Flow

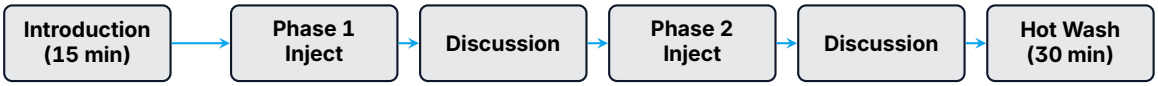

Figure 3: Typical tabletop exercise flow

6.2 Facilitation Tips

- **Stay neutral** – Don't lead participants to "correct" answers
- **Encourage participation** – Draw out quieter team members
- **Manage time** – Keep discussions focused, use parking lot for tangents
- **Capture insights** – Assign a note-taker for key decisions and gaps
- **No blame** – Focus on process improvement, not individual criticism

6.3 Key Discussion Questions

For each scenario phase, ask:

- Who needs to be notified? When?
- What information do we need to make decisions?
- What are our options? Trade-offs of each?
- At what point do we isolate OT systems?
- How do we maintain safe operations during response?
- What if this happens during a critical production period?

7 After-Action Review

7.1 Hot Wash

Immediately after the exercise, conduct a brief debrief:

- What went well?
- What was confusing or unclear?

- What gaps did we identify?
- What needs immediate attention?

7.2 After-Action Report

Document findings formally:

Section	Content
Executive Summary	Key findings and recommendations
Exercise Overview	Objectives, scenario, participants
Strengths	What worked well, validated capabilities
Areas for Improvement	Gaps identified, with specific examples
Recommendations	Prioritized action items with owners

Table 4: After-action report structure

Key Point

The value of a tabletop exercise is in the improvements that follow. Track action items to completion and incorporate lessons learned into updated plans and procedures.

8 Exercise Frequency

Exercise Type	Frequency	Purpose
Basic tabletop	Quarterly	Maintain awareness, test updates
Cross-functional	Semi-annually	IT/OT coordination
Executive-level	Annually	Strategic decisions, resource allocation
Full-scale (if feasible)	Every 2–3 years	Validate end-to-end capabilities

Table 5: Recommended exercise frequency

9 Summary

Key Takeaways

- **Safe Testing:** Tabletop exercises allow testing OT incident response without operational risk
- **Include OT Staff:** Operations and engineering must participate; decisions affect physical processes
- **Realistic Scenarios:** Base exercises on actual threats to your industry and systems
- **Structured Approach:** Progress through detection, containment, eradication, and recovery phases
- **Document Outcomes:** Capture gaps and improvements in after-action reports
- **Follow Through:** Track action items to completion; exercises without follow-up waste effort

10 Further Reading

Government Resources

- **CISA Tabletop Exercise Packages** – Ready-made exercises for critical infrastructure
  https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages
- **FEMA Homeland Security Exercise and Evaluation Program** – Exercise design guidance
  https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep

Standards

- **NIST SP 800-84** – Guide to Test, Training, and Exercise Programs
  https://csrc.nist.gov/pubs/sp/800/84/final

Books

- Bodeau & Graubart – *Cyber Resiliency Engineering Framework* (MITRE)
- Cichonski et al. – *Computer Security Incident Handling Guide* (NIST)

Part of the OT Security Learning Series