Running a Tabletop Breach Exercise Under Contract Performance

### Purpose of this Exercise

This exercise is designed to help Contracting Officers (COs) and Contracting Officer’s Representatives (CORs) practice their roles in responding to a cloud service breach under an active contract. The activity simulates a real-world incident to test coordination, response protocols, and alignment with contract terms.

This is a performance-focused exercise, not a compliance audit. The goal is to uncover gaps, clarify roles, and build readiness before an actual breach occurs.

### **When to Use**

Recommended use cases include:

* As part of quarterly or semiannual contract performance reviews
* When onboarding a new CO, COR, or contractor team
* Prior to executing a contract modification involving security clauses
* After updates to agency breach notification or incident response policies

### **Learning Objectives**

By the end of this exercise, participants should be able to:

* Apply contract breach clauses in a time-sensitive, real-world context
* Clarify roles and escalation responsibilities across government and vendor teams
* Identify weaknesses in documentation, workflows, or communication paths
* Strengthen response readiness and documentation protocols

### 

### 

### **Materials Needed**

* Current contract, including breach response or incident clauses
* Relevant agency policies (e.g., FedRAMP, NIST 800-53, CJIS)
* Scenario handouts (printed or digital)
* Role-based breach response worksheets

### **Role Overview**

| **Role** | **Primary Responsibilities During Exercise** |
| --- | --- |
| CO | Ensure contract compliance, interpret clause applicability, and assess need for mod action |
| COR | Monitor performance, track documentation, validate vendor communication timelines |
| PO | Coordinate across delivery and vendor teams; assess impact to users and outcomes |
| Vendor | Detect, report, and remediate incident; provide status updates and root cause analysis |
| Security SME (optional) | Provide technical context and ensure alignment with agency-specific protocols |

### **Duration**

60 to 90 minutes. Time blocks can be adjusted based on available session length.

### **Exercise Agenda**

1. **Opening Briefing (5 minutes)** Introduce participants, present scenario overview, and outline expectations.  
    Reinforce that the purpose is collaboration, not compliance review.
2. **Initial Role Reactions (15 minutes)** Prompt: What would you do during the first six hours after breach discovery?  
    Each participant outlines their responsibilities, communications, and decision points.
3. **Scenario Update (10 minutes)** Share new detail: The breach is confirmed and affects 1,500 user records.  
    Prompt participants to reassess their role response.
4. **Updated Actions and Coordination (15 minutes)** Roles revise their actions based on updated information.  
    Explore how escalation, documentation, or scope of response changes.
5. **Joint Response Planning (15 minutes)** Facilitate a group planning session.  
    Prompt: What coordinated actions are needed across roles to respond effectively?  
    Document cross-functional response plan and identify key decisions.
6. **Debrief and Lessons Learned (15–20 minutes)** Facilitate discussion on what worked, what broke down, and what needs to change.  
    Prompt: Where did delays, misunderstandings, or risk exposure occur?

### Scenarios for Tabletop Use

The facilitator may select one scenario or run multiple rounds using different examples.

**Scenario 1: Delayed Notification**A contractor-managed cloud platform detects unauthorized access to log files at 3:00 AM. The vendor delays notifying the government until 10:00 AM due to uncertainty about escalation procedures and concern about over-reporting. The exposure window remains unclear.

**Scenario 2: COR on Leave**A vendor discovers that a misconfigured storage bucket has been publicly accessible for over a week, potentially exposing sensitive audit records. The COR is on leave for two weeks, and no backup contact was designated. The vendor sends an email but receives no reply and does not escalate.

**Scenario 3: Internal Staff Breach**An agency staff member with privileged access logs into the vendor’s dashboard after hours and downloads sensitive PII. The vendor detects the activity but delays reporting, unsure whether it was authorized. Two days pass before clarification is reached.

### **Scenario 4: Partial Data Exposure with Ambiguous Scope**

A vendor supporting a shared-service platform discovers that due to a configuration error, access control policies were not applied correctly across tenant environments. An internal audit reveals that external users may have been able to see portions of system configuration logs. It is unclear whether the logs contain any user data or if access was actually exploited

**Scenario 5: Misrouted Incident Response** A junior vendor developer detects unusual log traffic and follows internal procedures to report it. Due to a routing error, the alert goes to the agency’s Tier 1 help desk instead of the COR or security team. No escalation occurs for 48 hours, during which the breach expands.

### **After-Action Items**

Facilitator should document:

* Specific process or policy gaps identified during the exercise
* Opportunities to improve contract clause clarity or response timelines
* Recommended training or follow-up with vendor or internal stakeholders
* Draft checklist or playbook revisions based on discussion

### **Optional Templates and Tools**

* Breach response worksheet (by role)
* Summary sheet of applicable contract clauses
* Escalation diagram with alternate contacts
* Notification timeline tracker

### **Facilitation Tips**

* Use plain language and link actions back to the contract
* Encourage real-world anecdotes to ground the discussion
* Reinforce the CO’s oversight role, not as technical lead, but as authority over contract scope and performance
* Create a psychologically safe space, participants should feel comfortable identifying real vulnerabilities