COR/CO Guide: Running a Tabletop Breach Exercise Under Contract Performance

## **Purpose**

This guide is designed to help Contracting Officers (COs) and Contracting Officer’s Representatives (CORs) facilitate a tabletop breach exercise as part of ongoing contract oversight and performance monitoring. Modeled after disaster recovery planning exercises, this activity ensures that roles, responsibilities, and response protocols are well understood and tested in advance of an actual incident.

This is not meant to be a finger-pointing exercise but rather a root cause analysis of current processes that can impact security.

## **When to Use**

* During post-award administration as part of performance management
* In preparation for or review of a contract modification involving security clauses
* Following updates to agency breach or incident response policies
* After onboarding a new PO, COR, CO, or vendor team
* As part of a quarterly or semiannual operational check-in

## **Objectives**

- Reinforce contractually defined breach notification procedures  
 - Clarify roles across government and vendor teams during a security incident  
 - Identify documentation gaps or misunderstandings  
 - Practice clear communication and escalation processes  
 - Build readiness for real-world cyber incidents

## **Exercise Setup**

Participants: CO, COR, PO, Vendor Lead, Security SME (if available)  
 Time: 60–90 minutes  
 Materials:  
 - The contract’s breach and incident response clauses  
 - Agency breach notification policy (e.g., FedRAMP, NIST, CJIS if applicable)  
 - Scenario handout  
 - Breach response worksheet for each role

## **Role Assignments**

| **Role** | **Focus** |
| --- | --- |
| CO | Contract language enforcement, legal implications, modification authority |
| COR | Performance tracking, timeline validation, documentation review |
| PO | Risk to delivery, user impact, coordination with technical teams |
| Vendor | Detection, reporting, root cause analysis, remediation plan |
| Security SME | (Optional) Adds realism and guidance on agency-specific requirements |

## Exercise Flow

1. Briefing (5 min): Facilitator shares scenario and exercise goals.  
 2. Initial Reaction (15 min): Each role outlines what they would do within the first 6 hours of discovery.  
 3. Update #1 (10 min): Facilitator shares that the breach is confirmed and involves 1,500 user records.  
 4. Second Round (15 min): Each participant updates their role's response, coordination needs, and concerns.  
 5. Group Response Planning (15 min): Develop a joint incident response plan.  
 6. Debrief (15–20 min): Identify where coordination failed and what needs improvement.

After-Action Items

- Document lessons learned and recommendations  
 - Review contract breach clauses and revise if needed  
 - Identify training needs for agency or vendor staff  
 - Create a follow-up checklist for ongoing monitoring

## 

## **Optional Tools & Templates**

- Breach response worksheet  
 - Contract clause summary  
 - Escalation path diagram  
 - Notification timeline tracker

This exercise is a proactive tool to ensure contract readiness, foster transparency, and build stronger government-vendor collaboration in the event of a security breach.

## **Sample Scenarios**

### **Scenario 1: Delayed Notification**

A contractor-managed cloud platform supporting a benefits application detects unauthorized access to log files that include session tokens and metadata. The incident is flagged by the vendor’s monitoring tools at 3:00 AM, and their internal team initiates triage. However, due to unclear escalation procedures and fear of over-reporting, they wait until 10:00 AM to notify the government. The data exposure window remains uncertain.

### **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, who is the primary point of contact for performance oversight, is on scheduled leave for two weeks, and no alternate contact was provided. The vendor sends an email to the COR but receives no reply and is unsure how to escalate.

### **Scenario 3: Internal Staff Breach**

An agency staff member with privileged access to the vendor's cloud dashboard logs in after-hours and initiates several unauthorized queries that result in mass downloads of personally identifiable information (PII). The vendor detects the anomaly but hesitates to report it, unsure whether the activity was authorized. By the time clarification occurs, two days have passed.

### **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 developer at the vendor site notices suspicious log traffic and flags it as a potential breach. They follow internal procedures and submit a security incident ticket. However, due to incorrect routing rules, the alert goes to the agency’s Tier 1 help desk instead of security or the COR. The help desk does not escalate it for 48 hours. Once discovered, the scope of the breach has expanded.