

TPRM Tabletop Exercise Template

Vendor Incident Response Scenario | Facilitator and Participant Guide

Available at www.tpvrm.net/documents | *The Future of Third-Party Risk Management & Data Privacy*

EXERCISE OVERVIEW

Exercise Name	[Insert Exercise Name]
Date	[Insert Date]
Duration	3-4 hours (adjustable)
Facilitator	[Insert Facilitator Name and Title]
Participants	TPRM Team, Legal, Information Security, Privacy, Procurement, Business Unit Representatives, Executive Sponsor (optional)
Classification	CONFIDENTIAL - FOR EXERCISE PURPOSES ONLY

Note: The fictional vendor names used in this scenario (DataFlow Analytics, CloudSecure Corp) do not represent any real organizations. Adjust the scenario details to match the characteristics of actual Tier 1 vendors in your portfolio, without using real vendor names in the exercise.

EXERCISE OBJECTIVES

This tabletop exercise aims to assess and enhance the organization's capability to respond to a major vendor security incident. Participants should understand by the end of the exercise:

- The process an organization follows in response to a vendor incident notification
- The roles and decision-making authority of each participating function
- The rights and obligations under the contract triggered by a vendor breach
- The regulatory notification requirements that may occur
- Gaps in incident response processes, contractual clauses, or communication protocols

SCENARIO BACKGROUND

Read aloud or hand out to participants at the start of the exercise. Do not share scenarios beforehand.

MASTER SCENARIO EVENT LIST (MSEL): DATAFLOW ANALYTICS INCIDENT

DataFlow Analytics (fictional) is a SaaS platform your organization uses for customer analytics, data aggregation, and reporting. Under your contract, DataFlow processes customer names, email addresses, transaction histories, and behavioral profiles for about 400,000 of your customers. DataFlow is classified as a Tier 1 vendor in your TPRM program. Your organization signed a Data Processing Agreement (DPA) with DataFlow 18 months ago.

DataFlow stores your data in a shared cloud environment with over 60 other enterprise clients. Your contract includes a 72-hour breach notification requirement, a right to audit, and a prohibition on using your data to train AI models.

INJECT 1: Initial Notification (T+0)

Friday at 4:45 PM, your TPRM team receives an email from DataFlow Analytics' Chief Security Officer with the subject line: "Important Security Notice - Potential Data Exposure." The email states that DataFlow has detected "anomalous access patterns" affecting its production environment and is "investigating a potential security event." It does not specify which clients are affected, describe the nature or scope of the exposure, and asks you to "stand by for further information."

#	Discussion Question	Expected Response / Key Points	Facilitator Notes
1	Who needs to be notified immediately within your organization?	TPRM Lead, CISO, Legal, Privacy Officer, and the business unit that owns the DataFlow relationship. Escalation chain should be documented in incident response procedures.	Ask: Does a documented escalation matrix exist? Who has the authority to declare a vendor incident?
2	What contractual rights can you invoke right now?	Review DPA for notification obligations, right to request status updates, right to audit, right to restrict processing, right to data inventory. Check 72-hour notification SLA.	Ask: Do participants know where to find the contract and DPA? Is there a contract repository?
3	What information do you need from DataFlow within the next 24 hours?	Nature of the incident, systems and data types affected, scope (which clients), timeline of events, containment measures taken, and whether a forensic investigation is underway.	Ask: Does your vendor notification policy require a specific format or content for incident notifications?

INJECT 2: Scope Confirmation (T+36 hours)

Monday morning. DataFlow issues a second notification confirming that a ransomware attack encrypted some of its production servers over the weekend. DataFlow confirms that your organization's customer data, names, email addresses, and transaction histories for about 380,000 customers were accessed by the attacker before encryption. DataFlow states it has contained the attack and is working with a forensic firm. DataFlow has not yet notified regulators.

#	Discussion Question	Expected Response / Key Points	Facilitator Notes
4	What are your regulatory notification obligations and timelines?	GDPR 72-hour notification to DPA if EU residents affected. State breach notification laws (California, New York, etc.) based on resident location. FTC Safeguards Rule if applicable. Assess which laws apply based on customer geography.	Ask: Who owns regulatory notification decisions? Does legal have a current breach notification checklist?
5	DataFlow has not notified regulators. Does your organization need to act independently?	As data controller, your organization may have independent notification obligations regardless of what	Ask: Does the DPA clearly assign controller notification responsibility? What does your contract say?

#	Discussion Question	Expected Response / Key Points	Facilitator Notes
		the processor does. You cannot wait indefinitely for DataFlow to act. Engage legal to assess controller obligations.	
6	Should you suspend DataFlow's access to your data or terminate the relationship?	Assess: can DataFlow still process data safely? Does containment appear sufficient? Suspension and termination rights in contract. Business impact of suspension. Alternative vendor options.	Ask: Does the contract include a suspension right without termination? What is the cure period?
7	What is your customer notification strategy?	Notification obligations by state/jurisdiction. Timing and content of notice. Credit monitoring obligation. Designated communication channel. Legal review of notice content. Coordination with DataFlow on joint vs. separate notification.	Ask: Is there a pre-drafted breach notification template? Who approves customer communications?

INJECT 3: Complication (T+72 hours)

A privacy advocacy group posts on social media that it has found evidence of the DataFlow breach and names your organization as one of the affected clients. Media inquiries start pouring in. Meanwhile, DataFlow tells you that its forensic investigation suggests the attacker may have stolen data for up to 90 days before it was discovered.

#	Discussion Question	Expected Response / Key Points	Facilitator Notes
8	How do you handle inbound media inquiries?	Designate single spokesperson. Prepare holding statement. Do not confirm or deny breach scope until investigation is complete. Coordinate with Legal and Communications.	Ask: Who is authorized to speak to media? Is there a crisis communications protocol?
9	Does the 90-day exfiltration window change your legal and regulatory analysis?	Potentially expands scope of affected data. Extends notification obligations. May implicate prior billing cycles or other data sets not initially identified. Triggers re-assessment of contract SLAs (was continuous monitoring in place?).	Ask: Does your monitoring program include real-time alerting for vendor anomalies? Would this have been detected sooner?
10	What long-term contractual or vendor relationship decisions need to be made?	Root cause analysis required from DataFlow. Contract remediation: enhanced monitoring, audit, penalty provisions. Evaluate vendor replacement. Document risk acceptance decision if continuing relationship. Update TPRM risk register.	Ask: What does the contract say about remediation obligations and cure periods? Do you have an exit plan?

DEBRIEF GUIDE

After completing the scenario, conduct a structured debrief. Allow approximately 45-60 minutes.

Lessons Learned Capture

What Worked Well	Gaps Identified / Improvement Actions

Action Items

Action Item	Gap Addressed	Owner	Due Date

Exercise Facilitator Sign-Off	
After-Action Report Due	