

# Tabletop after-action report (sample)

Sanitized excerpt • Evidence ID: IR-004

## Scenario

Phishing leading to workforce account takeover. Objective: validate detection, containment, escalation, and communications under time pressure.

## What worked

Clear incident commander ownership. Containment steps were approved quickly. Internal comms cadence was defined early and followed.

## Gaps (summary)

Two gaps were identified: (1) logging retention ownership unclear, (2) customer holding statement template missing. Both gaps were converted into owned remediation items with due dates.

# Remediation follow-through (sample)

Owned actions and proof expectations • Evidence ID: IR-010

## Remediation items

LOG-001: assign retention owner and capture retention export quarterly (due 2026-02-01).

COMMS-001: create and approve customer holding statement template (due 2026-02-01).

## Definition of done

Each item is closed only when proof exists (export, approved template, or runbook update). Closure without evidence creates buyer follow-ups later.