Cloud remediation closure record

One finding, one defined scope. Close only when both security and required service checks pass with current evidence. Missing evidence or a service regression keeps the case open.

Finding / asset / environment

Owner / reviewer / date

Business impact and required service behavior

Exposure and working service baseline evidence

Approved action, revision, expiry, and preconditions

Execution receipt and observed target state

Security retest: identity, method, time, result, evidence

Service check: identity, method, time, result, evidence

Evidence source, collector, and separation from executor

Unresolved risk, evidence gaps, and coverage limits

Decision and reason: close, open, or inconclusive

Reopen trigger, next action, and responsible owner

Keep the underlying observations, approval, and receipts in a controlled evidence store; use references here. A passing canary check supports only the recorded asset, access path, and time. It does not establish the absence of earlier access or the health of every service operation.