



THE MULTI-CLOUD RECOVERY READINESS PLAYBOOK

30 questions to test your recovery readiness.

Bring evidence to your next resilience review.

A practical question bank for CISOs, backup and DR leaders, cloud architects, and partners serving AWS, Azure and Google Cloud estates.

30

REVIEW
QUESTIONS

6

RECOVERY
DOMAINS

1

WORKSHOP
WORKSHEET

3

PARTNER
ENGAGEMENTS

FOR ENTERPRISE TEAMS AND CLOUD SERVICES PARTNERS

WHY THESE QUESTIONS MATTER

A backup report starts the conversation. Recovery evidence moves it forward.

Use this guide to identify what is known, what remains untested, and which gap deserves an owner next.

A successful job, an assigned policy and a stored copy each answer a useful question. A recovery decision also needs the workload, the failure scenario, access dependencies, and evidence that the required outcome can be achieved.

STARTING SIGNAL	EVIDENCE TO REQUEST
The backup job completed.	The restore result, validation scope and measured recovery time.
We have several copies.	Where they reside and which identities, keys or services they share.
The copy is immutable.	The lock mode, retention state and permissions that could affect it.
The finding was closed.	The before-and-after state and the check that verified closure.
Storage looks orphaned.	Its lineage, owner, dependencies and retention obligations.

WORK WITH THE STACK YOU ALREADY HAVE

Separate configuration issues, failed processes, missing evidence and genuine capability limits. Use the diagnosis to choose a response with your backup providers.

Forttic's Continuous Resilience Enforcement (CRE) loop connects Discover, Assess, Enforce, Verify and Report. Across supported, connected backup systems, it brings assessment, remediation within guardrails and recovery verification into one operating process. Use this guide to define the evidence your team or client needs from that process.

USING THE QUESTION BANK

Start with one service. Leave with one evidence-backed plan.

Run a 45-minute discussion with the service owner, backup or DR lead, cloud architect and security representative.

01

Define the scenario

Name the service and recovery objective. Choose a scenario: deletion, compromised admin access, regional outage or failed restore.

02

Ask six opening questions

Start with Q01, Q06, Q11, Q16, Q21 and Q26. Expand only where the answers expose a decision or uncertainty.

03

Record the evidence status

Use E for evidenced, G for a confirmed gap, U for unknown, or N/A with a documented reason. A missing observation is not proof that a backup is absent.

04

Assign the next step

Name an owner, a due date and a verification criterion. Take the three most consequential items into the worksheet on page 10.

WHAT COUNTS AS EVIDENCE?

Record the source, timestamp, workload scope, test conditions and result. A configuration check, a sample restore and a full service exercise establish different things.

RPO: acceptable data loss expressed in time. RTO: target time to restore the required service. This guide supports discussion and prioritization; it is not a certification, audit opinion or recovery guarantee.

Q01-05 / 5 QUESTIONS

01 Estate and coverage

Build a reconciled view of what needs protection and where the recovery copies actually live.

USE IN Discover / assessment

LANDS WITH Cloud architects, backup administrators

01 Which critical workloads lack a discovered backup or an assigned protection policy?
Evidence to request: Reconciled workload and backup inventories, scope exclusions and visibility limits.

02 Which backup jobs or vaults were created outside the approved process?
Evidence to request: Creation events, responsible identities, account or project, and monitoring status.

03 Where does each workload write its backup copies across clouds and vendors?
Evidence to request: A workload-to-copy map with location, protection tool, account and target.

04 Which copies share storage, identity, key or control-plane dependencies?
Evidence to request: A dependency map that distinguishes copy count from failure independence.

05 What changed in the protection estate since the last review?
Evidence to request: Added, removed and modified assets, timestamps and accountable owners.

CAPTURE THE ANSWER

Status: E / G / U / N/A | Evidence link + date | Owner + next action

Q06-10 / 5 QUESTIONS

02 Exposure and policy drift

Prioritize findings by the service at risk and the recovery options that remain.

USE IN Assess / risk review

LANDS WITH CISOs, security and resilience leaders

06 If a backup admin identity is compromised, which copies could it alter or delete?

Evidence to request: Effective permissions, reachable repositories and independently accessible options.

07 Which workloads have recovery points older than their declared RPO allows?

Evidence to request: Usable recovery-point timestamps, copy lag and each workload's RPO.

08 Where has retention drifted from the approved requirement?

Evidence to request: Approved policy, observed settings, change history and approved exceptions.

09 Which immutable copies have settings or permissions that weaken the intended protection?

Evidence to request: Lock mode, retention status, privileged access and relevant change events.

10 Where do equivalent recovery requirements receive different protection across clouds?

Evidence to request: A requirement-to-control comparison with resource-specific limits and gaps.

CAPTURE THE ANSWER

Status: E / G / U / N/A | Evidence link + date | Owner + next action

Q11-15 / 5 QUESTIONS

03 Action and verified closure

Make the boundary between automatic action and human approval explicit.

USE IN Enforce / remediation

LANDS WITH Platform owners, change approvers

11 When a critical backup job stops, who owns the response and what happens next?

Evidence to request: Detection record, assigned owner, approved response and completion status.

12 Which changes can run within guardrails, and which require approval?

Evidence to request: Action allow-list, permission scope, approval rules and escalation path.

13 Which remediation actions are blocked or waiting for approval, and why?

Evidence to request: Pending actions, accountable approvers, age and the reason work has stopped.

14 Can we trace an approved change to the resulting protection state?

Evidence to request: Before-and-after settings, approval, execution log and affected resources.

15 What evidence must exist before a protection finding is closed?

Evidence to request: A defined closure criterion, post-change check and result linked to the finding.

CAPTURE THE ANSWER

Status: E / G / U / N/A | Evidence link + date | Owner + next action

Q16-20 / 5 QUESTIONS

04 Restore and service recovery

Match the strength of the evidence to the recovery claim you need to make.

USE IN Verify / exercise

LANDS WITH DR engineers, application owners

16 When did this critical service last pass a recovery test, and what exactly was tested?

Evidence to request: Scope, date, identity, environment, validation result and measured RTO/RPO.

17 Which successful backup jobs were followed by failed restore tests?

Evidence to request: Linked job and restore results, failure cause and the response owner.

18 Which important copies have never been restore-tested, or have outdated evidence?

Evidence to request: A per-copy test record and the reason the evidence no longer fits the requirement.

19 Can the recovery team restore if the production account or region is unavailable?

Evidence to request: A tested supported path, independent access, keys and required dependencies.

20 Do measured recovery outcomes still meet current business objectives?

Evidence to request: Comparable test results, current targets and material changes since testing.

CAPTURE THE ANSWER

Status: E / G / U / N/A | Evidence link + date | Owner + next action

Q21-25 / 5 QUESTIONS

05 Copy lineage and storage purpose

Identify unnecessary spend without removing a required recovery option.

USE IN Discover / cost review

LANDS WITH Backup owners, FinOps, cloud partners

21 Which snapshots have no active source workload, and what is their recorded purpose?

Evidence to request: Source lineage, decommission date, owner and current storage cost.

22 Which retained copies are required for a hold, contract or approved retention policy?

Evidence to request: Recorded obligation, approving owner, review date and retention decision.

23 Which vendor or workflow created each copy, and who is accountable for it?

Evidence to request: Creation history, tool attribution and evidence supporting the ownership match.

24 What references or recovery dependencies would make a proposed deletion unsafe?

Evidence to request: Image and template references, sharing relationships and remaining recovery copies.

25 How much storage supports active protection, justified retention or unresolved ownership?

Evidence to request: Cost allocation methodology, attribution gaps and a reviewed cleanup candidate list.

CAPTURE THE ANSWER

Status: E / G / U / N/A | Evidence link + date | Owner + next action

Q26-30 / 5 QUESTIONS

06 Incident and executive evidence

Give decision-makers a bounded answer with the evidence and uncertainty attached.

USE IN Report / incident review

LANDS WITH CISOs, incident leads, audit stakeholders

26 If ransomware is suspected now, what recovery options can we substantiate?

Evidence to request: Candidate points, validation and threat-screening scope, timing and uncertainties.

27 If a backup vendor is disrupted, which services depend on it and what alternatives remain?

Evidence to request: Vendor-to-service dependencies and evidence for each alternative recovery path.

28 Can we show the chain from policy to action to verification for one critical workload?

Evidence to request: Linked policy, finding, approval, action and verification records.

29 What changed in recovery readiness over the last quarter, and which gaps remain open?

Evidence to request: Comparable scope, trend methodology, material events and accountable owners.

30 What can we tell the board today without overstating confidence?

Evidence to request: A dated summary of tested outcomes, open exposure, unknowns and decisions needed.

CAPTURE THE ANSWER

Status: E / G / U / N/A | Evidence link + date | Owner + next action

YOUR REVIEW WORKSHEET

Turn answers into next actions.

Complete this page for one service and one recovery scenario. Use the question numbers to keep the evidence traceable.

Service / business owner:

Scenario / assessment date:

RPO / RTO / scope:

EVIDENCE STATUS BY DOMAIN

Enter question numbers under each status. Count N/A only with a reason.

DOMAIN	E	G	U	N/A
Estate and coverage				
Exposure and policy drift				
Action and verified closure				
Restore and service recovery				
Copy lineage and storage purpose				
Incident and executive evidence				

TOP THREE DECISIONS

For each: question number + gap or unknown / owner + due date / evidence required to close.

1

2

3

E = evidenced for this scope. G = confirmed gap. U = unknown. N/A = not applicable with a reason. Do not average away a critical gap; prioritize by business impact and available recovery options.

FOR CLOUD AND BACKUP SERVICES PARTNERS

Make the review a repeatable service.

Use the same evidence questions across AWS, Azure and Google Cloud engagements, adapted to supported services and the client's requirements.

01

DISCOVERY / SCOPE THE WORK

Open with Q01, Q06, Q16, Q21 and Q26. Identify the service owner and request a small evidence sample before proposing changes.

Deliver: scoped gap register, visibility limits and agreed priorities.

02

REMEDIATION / VERIFY THE CHANGE

Use Q11-15 to establish approvals and closure criteria. Work with the client's existing cloud and backup providers on the appropriate remedy.

Deliver: approved change record, verification result and residual risks.

03

RECURRING REVIEW / KEEP EVIDENCE CURRENT

Revisit material changes, untested copies and overdue actions. Use Q28-30 to translate the results into a sponsor-ready review.

Deliver: refreshed evidence pack, trend with consistent scope and next decisions.

AGREE THE DELIVERY BOUNDARY

Name the customer approver, partner operator, cloud or backup provider responsibilities, and Forttic integration scope. This guide does not imply a formal partner authorization or guaranteed service outcome.



TAKE THE NEXT STEP

Bring five questions. Choose one workload. Define the proof.

Explore a recovery readiness briefing with Forttic.

1

Bring your priority scenario

Choose a critical service, its recovery targets and the disruption you need to withstand.

2

Review the evidence and integration scope

Use your question shortlist to discuss current visibility, supported systems and the checks that matter.

3

Agree the next action and verification

Decide what to investigate or change, who approves it, and how the outcome will be established.

Discuss your recovery readiness review

hello@forttic.com | forttic.com

About this guide: adapted from Forttic's CRE validation questions into workshop prompts. It does not certify implementation of every scenario. Confirm supported integrations and validation scope with Forttic.

Framework: forttic.com/features/cre-framework.html