FACILITATED TABLETOP EXERCISE

Run a 30-minute response exercise with the people who would actually be in the room.

This pack is a discussion aid, not an emergency plan, compliance assessment or substitute for organisation-specific procedures.

Scenario

09:14. A primary customer identity service becomes unavailable. Customers cannot sign in. The cause is unknown. Monitoring shows a sharp increase in authentication failures, but the affected regions and duration are not yet confirmed.

Facilitator stages

1 - Declare	Who can declare an incident? What minimum facts are required? Who needs to know immediately?
2 - Establish command	Who is incident commander? Which technical, operations, communications and executive roles are needed?
3 - New evidence	A configuration change is suspected but not verified. How does the team prevent an assumption becoming a fact?
4 - Response proposal	A secondary authentication path may reduce impact. Who can recommend it, who must approve it and who executes it?
5 - Handover	The current commander must leave. What does the next shift need to receive in a frozen handover?
6 - Review	Which facts, decisions, delays and unresolved questions should carry into the post-incident review?

ROLE LENSES

Ask the same incident from four different seats.

The exercise becomes more useful when each participant answers from their actual responsibilities rather than from an idealised “incident team” perspective.

Incident commander	What do you need to know now? Which role is missing? What decision is blocked and why?
Operations lead	What customer or operational impact can you confirm? Which workaround creates a new risk?
Security lead	Which evidence supports the suspected cause? Which assumption must remain explicitly unverified?
Executive	What is the business impact, what decision needs escalation, and what can be communicated with confidence?

Debrief prompts

- Where did ownership become ambiguous?
- Which fact would have been hardest to verify?
- Which decision needed a clearer approval boundary?
- What information would the next shift struggle to reconstruct?
- What should be changed before the next incident?

KEEP THE EXERCISE HONEST
Do not turn the scenario into a test of one person. The goal is to expose unclear handoffs, missing information and authority boundaries before a real event does.

Try the interactive version at criticl.com.au/exercise