

Incident readiness discussion guide

Run a short discussion about authority, contacts, continuity, communication and evidence after an incident.

Purpose

Use a 45-60 minute facilitated discussion to find decision and coordination gaps. The scenario is a suspected account compromise followed by a critical service becoming unavailable; no attack simulation or technical intrusion is required.

Prepare before the discussion

- Leadership, IT, the service owner and the relevant program or operations representative.
- Protected incident contacts, provider responsibilities and the current continuity plan.
- A facilitator, a note taker and an agreed discussion boundary.

Review prompts - first half

1. Set the exercise boundary

Use an invented organization and synthetic records. Confirm this is a discussion exercise, not a production change, and name the facilitator and decision owner.

2. Introduce the first report

A staff member reports an unexpected sign-in notice. Who receives the report, records the facts and decides whether to escalate?

3. Check authority to act

Who may restrict access or pause a service? Identify what requires leadership approval, what the provider can do and how business impact is considered.

4. Introduce the service outage

A critical application is unavailable. Which work must continue, which approved alternate process is used and who confirms that the alternate is safe?

5. Protect people and sensitive records

Where children's programs or sensitive services are involved, who owns safeguarding decisions and the protected record-access process during the outage?

Review prompts - continued

6. Preserve useful evidence

Agree who preserves relevant logs and records without altering or broadly sharing them. Identify the protected evidence location and specialist escalation route.

7. Coordinate external responsibilities

Identify provider, insurer, legal and other required notification decisions. Confirm responsibilities and applicable deadlines with qualified advisers rather than improvising them in the exercise.

8. Plan communication

Who approves messages to staff, volunteers, affected people and the public? Establish an alternate contact route if normal email is unavailable.

9. Agree recovery acceptance

Who confirms a service is ready to resume? Consider authorized access, useful data, important dependencies and the approved recovery plan.

10. Close with owned actions

Record decisions, unknowns and the three most useful improvements. Assign an owner, a due date and a check that shows the coordination gap has been addressed.

Useful outputs

- An exercise record separating hypothetical discussion from observed operating evidence.
- Confirmed decision authority, alternate contacts and continuity responsibilities.
- A small action register and a date to verify the improvements.

Review prompt

Repeat after significant team, provider or critical-service changes and on an agreed exercise cadence.

Your next decisions

Use this worksheet in your approved protected workspace. Record categories and decisions, not personal records, passwords, card data or recovery codes.

Scope / systems / programs: _____

Review owner: _____ Review date: _____

Topic / gap	Evidence / unknown	Owner / next action	Due / completion check

Where Layer8 can help

Cybersecurity: Assess the authorized scope, prioritize improvements and verify agreed safeguards.

Scope and use

This discussion does not authorize containment or changes in a live environment. Specialist incident response, legal notification and continuous response coverage require their own agreed scope.

Original Layer8 preparation prompts. Linked reference organizations do not endorse this guide.

Primary references

CISA: small and medium business resources

<https://www.cisa.gov/small-and-medium-sized-business-resources>

NIST: small-business CSF quick-start guide

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf>

Online edition: [Layer8 resource library](#) / [incident-tabletop](#)