Incident and Continuity Tabletop Workbook

A 60-minute discussion about decisions, communications and keeping essential work going during a fictional service interruption.

Exercise boundary

Discuss only. Use fictional details. Do not attack systems, change access, disable services, restore live data or send messages to customers. Technical tests require separate authorisation and planning.

Essential business activity and the first serious consequence if it stops

Tolerable interruption and acceptable data-loss assumptions to validate

Role	Name / agreed responsibility
Facilitator / note-taker	
Business decision-maker	
Technology / provider contact	
Customer communications	

A sole operator can take the roles in turn and identify where outside help is needed. Agree provider participation in advance. Keep a protected contact route independent of the main email account.

Source guidance

NIST SP 800-61 Rev. 3, Incident Response Recommendations (3 April 2025)
https://csrc.nist.gov/pubs/sp/800/61/r3/final

NIST SP 1300, Small Business Quick-Start Guide (26 February 2024)
https://csrc.nist.gov/pubs/sp/1300/final

Original GRCPreneur design and examples. Sources inform the approach; no endorsement is implied.

Read these updates aloud

Scenario: shared files supporting an important business service are unavailable. Adapt the details to your chosen activity. The cause is initially unknown.

0-15 minutes | Uncertainty

Update: A device displays an unfamiliar message. The provider has not confirmed whether this is a security incident or a service fault.

Who receives the report and leads the response? What is known, assumed or unknown? Who contacts authorised technical help? Who can approve a containment action that interrupts work? Where are times and decisions recorded?

15-30 minutes | Continuing disruption

Update: Normal access will not return before noon. Two customer deadlines are approaching and the normal contact list is unavailable.

What reduced service can operate safely? Who approves it? Where will temporary information be protected? Which tasks must stop? What can customers be told without guessing, and when will they receive another update?

30-45 minutes | Possible recovery

Update: The provider proposes recovery from a copy that may not contain recent changes.

Who approves recovery? What evidence is needed? How will restored records be checked and temporary records reconciled? Who confirms the authoritative system? Does restored availability leave unresolved confidentiality or integrity questions?

45-60 minutes | Debrief and commitments

Select three achievable improvements. Assign an owner, due date and completion evidence to each. Record unresolved exposure in the risk register. Arrange a follow-up discussion after the actions are complete.

Keep routine service messages separate from any legally or contractually required notifications. Record who would obtain appropriate advice. This exercise does not establish a universal reporting deadline.

A tabletop tests discussion and coordination. It does not demonstrate that technical recovery works. Plan a separate, authorised restore test where appropriate.

Decision log

Exercise date: _____ Activity: _____

Distinguish a demonstrated capability from an assumption. Use the next review column for a checkpoint or an unresolved question.

Time	Known facts and uncertainty	Decision / action	Authority / owner	Next review

Do not put credentials, live incident evidence or personal customer information in this fictional exercise record.

Improve and recheck

Choose three actions the business can realistically complete. A useful action has observable completion evidence.

Finding / consequence	Agreed improvement	Owner / due date	Completion evidence

Unresolved exposure and the owner decision while improvement is pending

What will we rehearse again, with whom, and on what date?

Examples of meaningful completion

Demonstrate access to emergency contacts without the main email account. Agree the provider recovery assumptions in writing. Practise reconciling a small set of fictional temporary records.

Retain the workbook as a protected business record. It is general management guidance, not an emergency-response service, technical assurance or legal advice.