

Tabletop Exercise Pack

Six ready-to-run business continuity scenarios. Each takes about an hour and is designed to expose the assumptions in your plan before a real disruption does.

How to facilitate. Gather the people who would respond, plus a decision maker. Read the starting situation, then release each timed inject and pause for discussion. Nominate a note-taker. There are no trick questions; disagreement and hesitation are exactly what you came to find. Capture observations and improvement actions at the end, with owners and dates. Keep it no-blame.

Exercise 1 — No Office Monday

PURPOSE

Test your response to sudden, extended loss of premises.

STARTING SITUATION

It is 07:45 Monday. A burst water main has flooded the road and the landlord says the building will be inaccessible for at least three days. Some staff have laptops at home, many do not.

INJECTS

08:15 — Your largest customer expects today's orders confirmed by midday.

09:00 — Two of the three people who know the dispatch process are on holiday.

11:00 — A member of staff has driven in and is standing outside asking what to do.

DISCUSSION QUESTIONS

- What are our priority services this morning, and what is our minimum viable operation?
- Who can actually work, and what do the others need?
- How do we communicate with staff and customers?
- Can we reach the continuity plan and contacts without the office?

EXPECTED THEMES

- Home working depends on kit and access people may not have
- Key-person dependency on the dispatch process
- Offline plan and contacts matter

OBSERVATIONS / IMPROVEMENT ACTIONS

Exercise 2 — Microsoft 365 Down

PURPOSE

Test continuity when cloud productivity tools are unavailable (provider outage, not compromise).

STARTING SITUATION

Email, Teams and SharePoint are all unavailable. Microsoft reports a service incident with no restoration estimate. You have a major proposal due to a client at 16:00.

INJECTS

+30 min — Staff are asking whether it is safe to keep working, or whether this is a cyber attack.

+1 hr — The proposal files are in SharePoint and cannot be reached.

+2 hr — A customer emails your (unmonitored) inbox asking for an urgent update.

DISCUSSION QUESTIONS

- How do we communicate internally and with customers without Microsoft 365?
- How do we know this is an outage, not a compromise? Who decides?
- What work can continue, and what data will need reconciling later?

EXPECTED THEMES

- Alternative communications must exist in advance
- Distinguishing outage from compromise; route to Incident Response if in doubt
- Offline or alternative copies of critical documents

OBSERVATIONS / IMPROVEMENT ACTIONS

Exercise 3 — Internet Failure

PURPOSE

Test dependence on connectivity and your failover arrangements.

STARTING SITUATION

Your primary internet connection has failed. The carrier estimates restoration tomorrow afternoon. Phones are VoIP and card payments run over the network.

INJECTS

+15 min — Customers cannot get through on the phones.

+45 min — You discover your "backup" 4G router has a flat battery and no SIM data allowance.

+2 hr — Card payments are failing at the counter.

DISCUSSION QUESTIONS

- Is our second connection genuinely independent, and does it actually work?
- Can we reroute phones and take payments another way?
- What is our minimum viable operation on connectivity alone?

EXPECTED THEMES

- Untested failover is not failover
- Payment and phone dependencies on the same line
- Value of a diverse or mobile backup

OBSERVATIONS / IMPROVEMENT ACTIONS

Exercise 4 — Ransomware (continuity focus)

PURPOSE

Test how the business keeps operating during a cyber incident, while the Incident Response Plan handles the security side.

STARTING SITUATION

Files are encrypted across shared drives and a ransom note has appeared. IT has isolated affected systems and is following the incident response plan. You do not know yet how long recovery will take.

INJECTS

+1 hr — IT confirms you may be running on manual processes for several days.

+3 hr — Finance cannot access the accounting system; a supplier is chasing payment.

Day 2 — A customer asks publicly whether their data is safe.

DISCUSSION QUESTIONS

- What are our minimum viable services, and can we run them manually?
- How do we protect finance controls while systems are down?
- Who owns customer communication, and what do we say?
- Where does continuity end and incident response begin?

EXPECTED THEMES

- Two plans running in parallel: continuity keeps trading, incident response contains the threat
- Manual finance controls and payment verification
- Reconciliation planning for when systems return

OBSERVATIONS / IMPROVEMENT ACTIONS

Exercise 5 — Critical Supplier Collapse

PURPOSE

Test continuity of supply when a single-source supplier fails.

STARTING SITUATION

A supplier you rely on for a key component or service has gone into administration overnight, with immediate effect. You have limited stock.

INJECTS

+1 hr — You cannot reach anyone at the supplier; their phones are dead.

+3 hr — Your own customers have orders due this week that depend on this input.

Day 2 — A potential alternative supplier quotes a two-week lead time.

DISCUSSION QUESTIONS

- Which of our products or services does this affect, and how much stock buys us time?
- Do we have an alternative source, and who owns that relationship?
- Which customers do we prioritise, and what do we tell them?

EXPECTED THEMES

- Single-source supplier as a single point of failure
- Buffer stock and second-source arrangements
- Customer prioritisation and honest communication

OBSERVATIONS / IMPROVEMENT ACTIONS

Exercise 6 — Staff Shortage at Peak

PURPOSE

Test resilience to a high proportion of staff being unavailable during a busy period.

STARTING SITUATION

A winter illness has taken out around 40% of your staff, including two team leaders, during your busiest week of the year.

INJECTS

Morning — The person who normally runs dispatch is off, and nobody is quite sure of the full process.

Midday — Remaining staff are stretched and starting to make errors.

Day 2 — A key customer's large order is at risk.

DISCUSSION QUESTIONS

- What is our minimum staffing for priority services, and are we below it?
- Who can deputise, and is the critical work documented well enough for them to?
- What do we stop doing to protect the priorities?

EXPECTED THEMES

- Minimum staffing and deputies prepared in advance
- Documentation of key processes to reduce key-person risk
- Deliberately pausing non-priority work

OBSERVATIONS / IMPROVEMENT ACTIONS

Record lessons in the Continuity Improvement Register. See also the NCSC's free Exercise in a Box. Practical guidance, not legal advice.