

5-Point checklist for preparing an effective BCP scenario

A practical checklist for designing effective Business Continuity exercise scenarios.

Use this checklist to ensure your BCP scenarios are focused, realistic and deliver meaningful learning - not just assurance.

1. Define clear purpose, measurable objectives, and benchmarks

- **Action:** State explicitly what specific capabilities or mechanisms the scenario will stress-test, ensuring success criteria are tied to concrete performance metrics rather than simple attendance or process execution.
- **Example:** Instead of setting a vague goal like "Test IT incident response," define the objective as: "Evaluate the incident response team's capability to detect a ransomware infection, initiate core server isolation within 20 minutes, and invoke the secondary data center recovery protocol within 45 minutes."

2. Ground scenarios in high-impact, plausible priority risks

- **Action:** Select threat vectors derived from recent, real-world intelligence and internal risk assessments, balancing high severity with actual operational plausibility.
- **Example:** Model a primary cloud provider region outage occurring simultaneously with a targeted phishing campaign on key IT staff, rather than an improbable or generic catastrophe.

3. Engage the right roles and force cross-functional interaction

- **Action:** Involve key decision-makers across executive, legal, communications, operations, and IT functions, designing injects that actively require cross-departmental coordination and decision-making under pressure.
- **Example:** Present a scenario where customer data is potentially leaked, requiring legal to evaluate regulatory notification thresholds, PR to draft external statements, and operations to maintain core customer services concurrently.

4. Introduce dynamic pressure, escalation, and uncertainty

- **Action:** Structure time-bound injects and evolving updates that simulate real crisis friction, such as conflicting updates, missing information, and competing priorities, to evaluate decision-making under stress.
- **Example:** Inject a sudden social media leak about an ongoing system outage midway through the exercise, forcing the team to pivot resources toward public response while simultaneously attempting system diagnostic work.

5. Establish clear deliverables and convert insights into action

- **Action:** Require participants to produce tangible outputs during the exercise (e.g holding statements, executive briefing notes, action logs) and immediately capture learnings into a tracked remediation plan with assigned owners and fixed deadlines.
- **Example:** End the exercise with a structured post-mortem to document key gaps (e.g outdated escalation lists), then assign the Lead Continuity Planner to update and re-verify contact trees within 10 business days.