

Contacts and communication

Worksheet 1 of 4. Complete these fields with management, IT and operations. Keep a current copy in an agreed offline location.

Organisation / site: _____ Owner: _____
Version / next review: _____ Approved by: _____

Who takes responsibility

Role	Name and deputy	Verified contact and fallback
Coordination / lead	_____ _____	_____ _____
IT / IT provider	_____ _____	_____ _____
Operations / continuity	_____ _____	_____ _____
Facilities / safety	_____ _____	_____ _____

If email or phones fail

Approved fallback channel: _____
If that also fails, agreed meeting point: _____
Offline location of this pack and authorised users: _____
Last contact test / result: _____

Report and coordinate

For immediate danger, follow site safety and evacuation procedures and contact local emergency services when needed. Otherwise report what you observed, when, where and which activity is affected. Obtain acknowledgement; use the agreed deputy if no one responds. Do not improvise interventions on electrical or safety-critical systems.

Do not record passwords or recovery keys. Restrict distribution of personal contact details. Do not publish completed worksheets publicly.

Critical activities and continuity

Worksheet 2 of 4. Copy this sheet for each important activity. Timing estimates are planning assumptions to be agreed and checked with the responsible people.

Planning question	Your organisation's agreement
Activity and responsible person	
Impact on customers, people and operations	
When does disruption become unacceptable and why	
People, IT, data, premises and providers needed	
Minimum service and approved fallback process	
Who activates fallback operations and when they end	
Recovery target and conditions for authorisation	

Agree before resuming normal operations

Who confirms safety and availability? How will the service be tested? How will paper records and backlogs be reconciled without duplicate or missing transactions?

Having a backup does not establish that recovery will work. IT and operations should separately check data requirements, dependencies and tested recovery options.

A 30 minute team exercise

Worksheet 3 of 4. A discussion exercise using fictional information. Do not shut down systems, trigger real alerts or use customer data. A real incident ends the exercise.

Date: _____ Facilitator: _____ Recorder: _____

Participants / roles: _____

Time	Inject and questions
0–5 min	Agree the aim: test contact arrangements and one critical activity. Assign roles and confirm exercise rules.
5–15 min	09:10: Site power fails. ERP and office phones are unavailable. The cause is unknown. Who checks safety? Who coordinates? How does the team reach the deputy without email?
15–25 min	09:30: There is no reliable recovery estimate; mobile connections are unreliable. An important customer order is due. Which fallback process is authorised? What is paused? Who communicates with whom, and how?
25–30 min	Capture the three most important gaps. Assign an owner, a deadline and observable completion evidence to each.

Record observations

Question / decision	Observation or unresolved gap
_____	_____ _____
_____	_____ _____

To explore cyber scenarios, use the CyberDecisionLab tabletop generator. Select a suitable scenario; questions and notes from this worksheet are not transferred automatically.

[Tabletop generator](#)

Actions and next review

Worksheet 4 of 4. Close the exercise by recording results and assigning the next steps. Follow up to verify that the actions are implemented.

Gap and action	Owner / deadline	Evidence / status

Action follow-up date:
Who checks completion:
Next exercise and focus:

Keep the pack current

Review contacts, fallback channels and activities after changes and incidents, and agree a regular internal review date. Replace outdated offline copies. Mark an action complete only with evidence, such as a recorded contact test.

Use and sources

These original Paragamix GmbH templates may be used internally, adapted and shared with clients free of charge. A source link is welcome but not required. External materials retain their own terms.

[BSI – organisatorische Vorfallscheckliste](#) | [CISA – tabletop exercise materials](#)

Current version and sources

A starting point for organisational preparation. Not a complete continuity plan, technical authorisation or compliance certificate. Created with AI assistance; no independent expert approval of this kit is claimed. Have the responsible people review and approve it before operational use.