

Business Continuity Disaster Recovery Plan

Complete this plan to guide activation, continuity, technology recovery and return to normal after a disruption. Enter approved recovery objectives, authorities and verified contact references. Keep life-safety actions ahead of business recovery, and validate procedures through controlled exercises.

Complete bracketed fields with approved information. Duplicate modules and rows as needed; record the reason for any section marked not applicable.

Document [ID and revision] **Owner** [Role] **Scope** [Organization, site or product]

Effective date [Date] **Approval** [Controlled record] **Next review** [Date or trigger]

Plan overview and governance

Plan element	Approved arrangement
Purpose scope and objectives	[Sites, services, systems, exclusions and outcomes]
Assumptions and limitations	[Planning assumptions and situations outside this plan]
Phases and related plans	[Activation, recovery, reconstitution and stand-down; interfaces]
Ownership approval and distribution	[Role, approval record and controlled copies]

Business impact analysis and risk assessment

Activity or system	Impact and dependency	Approved recovery objectives
[ID and priority rationale]	[Impacts over time; upstream/downstream dependencies]	[RTO, RPO, tolerable disruption and units]
[ID]	[People, facility, supplier, data and minimum resources]	[Objective source and decision authority]
Threat or scenario	Assessment and current controls	Selected response
[Assessed disruption]	[Method, likelihood/impact and evidence]	[Strategy and decision record]

Continuity and recovery strategies

Dependency	Selected arrangement and capacity	Constraints and verification
[People, facilities or supplier]	[Workaround, alternate site or agreement]	[Prerequisite and exercise evidence]
[Technology and data]	[Backup, replication or recovery option]	[Verified objective and limitation]

Response structure

Team or role	Authority and responsibility	Alternate and handoff
[Declaration authority]	[Activate, escalate or stand down]	[Succession and decision record]
[Business or IT recovery team]	[Assigned restoration scope]	[Coordination and acceptance handoff]

Emergency response activation and notification

Activation stage	Approved action and responsible role	Decision or completion record
Life safety	[Protective action from the site emergency plan]	[Accountability and safe-entry status]
Assessment	[Incident, damage, impact and activation criteria]	[Facts and threshold comparison]
Declaration	[Authorized decision and scope]	[Time, authority and activation record]
Notification	[Verified order, channel and fallback]	[Sent, acknowledged and outstanding]

Crisis communications

Audience and trigger	Authority channel and message content	Timing and evidence
[Staff, customers or suppliers]	[Approver, verified channel, facts and required action]	[Adopted timing and delivery record]
[Regulator, media or emergency service]	[Authorized spokesperson and approved content]	[Applicable reviewed obligation and acknowledgement]

Situation update form

Record [incident ID], [verified time], [impact], [actions completed], [current constraints], [next decision] and [next update point]. Identify unconfirmed information explicitly.

Business continuity procedures

Repeat one module for each prioritized activity or site.

Activity setup	Approved continuity arrangement
Trigger priority and objective	[Entry condition, activity and recovery objective]
Resources and dependencies	[People, location, tools, supplier and access]
Reduced operation	[Workaround steps, capacity and service limitations]
Validation and records	[Minimum acceptable output, check and retained evidence]
Handoff	[Receiving process or team and acceptance]

IT disaster recovery

System recovery stage	Exact procedure or controlled reference	Validation and record
Entry and prerequisites	[Authorized trigger, dependency order and recovery environment]	[Ready state and approval]
Restore or fail over	[Verified recovery actions and backup/replication reference]	[Time, result and exception]
Validate	[Data integrity, function, access and service checks]	[Evidence against RTO/RPO]
Declare available	[Authorized acceptance and business handoff]	[Decision and remaining limits]

Reconstitution and return to normal

Return stage	Entry criterion and action	Authority and evidence
Prepare normal environment	[Safe site/system state and prerequisite]	[Readiness check]
Fail back and reconcile	[Controlled sequence, data reconciliation and rollback condition]	[Result and acceptance]
Stand down	[Declaration, notifications and temporary-resource cleanup]	[Decision and event record]

Exercises training and maintenance

Exercise or review	Objective scope and method	Results and follow up
[Activity, system or whole plan]	[Scenario, participants, criteria and adopted cycle]	[Observed gaps and evidence]
[Training or plan change]	[Audience, trigger and material]	[Completion and document update]

Post incident and exercise review

Objective or issue	Actual observation	Action and effectiveness check
[Recovery objective or decision]	[What happened, time and evidence]	[Owner, due date and retest]

Appendices

Resource or reference	Verified details	Owner and last check
[Contact directory or vendor agreement]	[Controlled location, role and fallback access]	[Verifier and date]
[Vital record, equipment or interconnection]	[Location, dependency, capacity and access]	[Verification evidence]
[Continuity term]	[Approved definition and units]	[Defining source]

Plan readiness review

- ☐ Recovery objectives, declaration authorities, contacts and dependencies are verified.
- ☐ Recovery steps and business acceptance checks were exercised; gaps remain visible.
- ☐ Controlled copies are accessible during the disruption conditions covered by the plan.

Reviewer role	Decision and date	Open gaps and approval reference
[Business, recovery or governance authority]	[Approved or returned]	[Record and next review trigger]