SOS / SAMPLE RECOVERY ENGAGEMENT

Know what must recover first.

Business continuity, disaster recovery and business impact analysis: a fictional supplier, sample network, recovery targets and completed deliverable examples.

Illustrative sample only

This document shows possible engagement outputs. It contains fictional assumptions, targets and exercise observations, not measured customer results, a fixed scope of work or a recovery guarantee. Actual recovery targets and acceptance criteria require business approval and technical validation.

Scenario

An 80-person engineering supplier loses its primary site at 10:00. The customer order process has a four-hour maximum tolerable interruption and a two-hour RTO. A separate warm standby receives application-consistent checkpoints. An approved manual order log supports continuity while IT recovers the service.

What the engagement connects

Business impact and critical assets → approved recovery targets → dependency-aware architecture and runbooks → measured exercises → improvement actions.

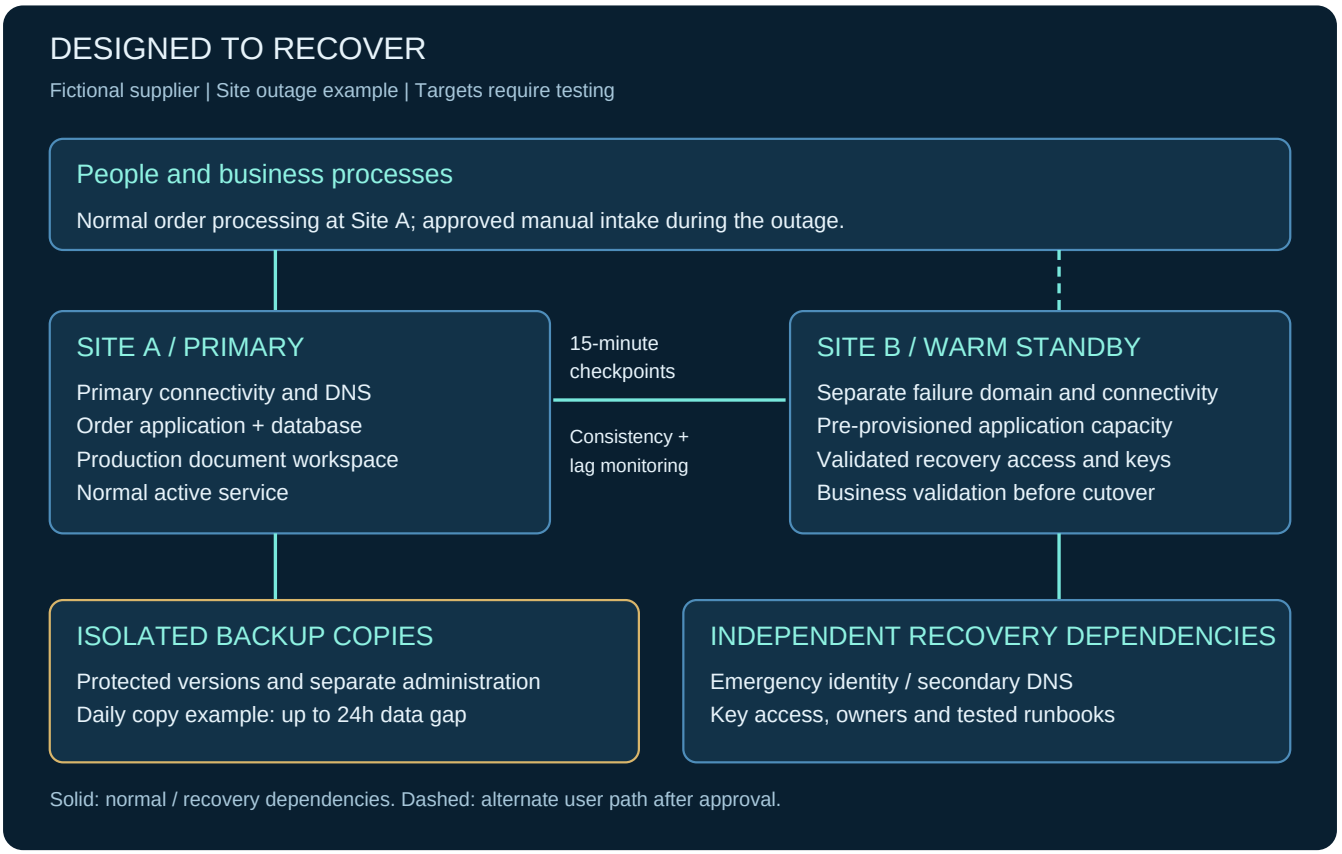
Possible deliverables

Business impact analysis; critical asset and dependency register; recovery network diagram; recovery runbook with owners and acceptance criteria; exercise report and improvement plan.

01 / ARCHITECTURE

A separate recovery path.

Warm standby capacity and isolated backups solve different problems. Neither is sufficient without tested access, clean data, business validation and accountable owners.



Design assumptions

Site B is pre-provisioned in a separate failure domain with secondary connectivity, DNS and licenses. Emergency identity recovery and encryption-key access do not depend solely on Site A. Capacity, geographic separation, security boundaries and data handling are reviewed against the organization's actual risks.

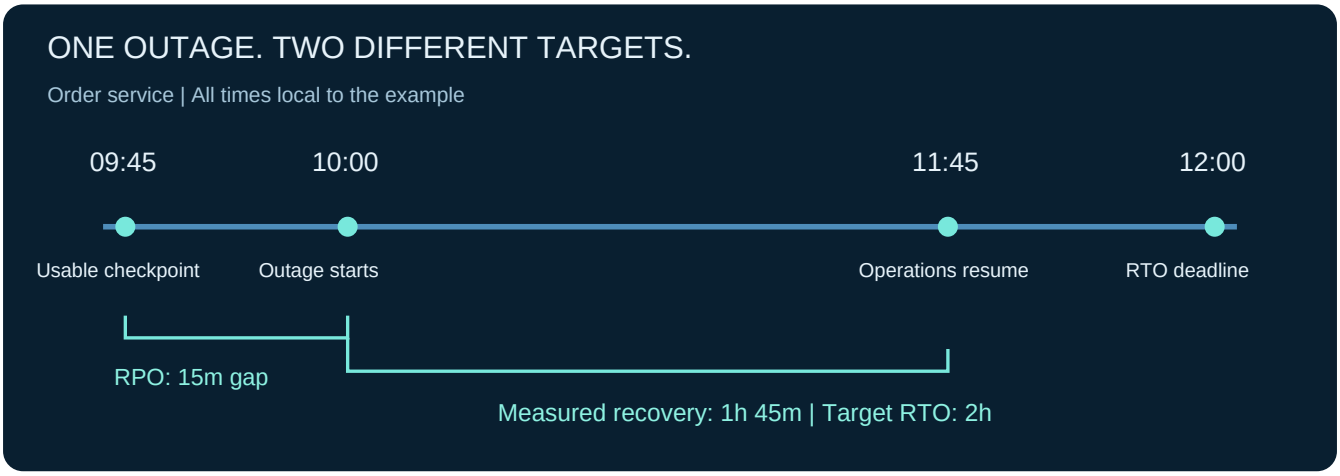
Replication is not a backup

Replication may copy corruption or deletion. The isolated daily backup example can have a 24-hour data gap, which does not meet the 15-minute order RPO if standby checkpoints are unusable. Reducing or accepting that gap requires an explicit decision.

02 / RECOVERY TARGETS

RPO looks back. RTO looks ahead.

Use business service timestamps, not the time a server powers on, to measure recovery.



Measure	Example	How it is verified
RPO target	15 minutes	Validate the latest usable checkpoint and any unrecoverable transactions.
Observed recovery-point gap	09:45 checkpoint to 10:00 outage = 15 minutes	Confirm consistency, checkpoint availability and reconciliation.
RTO target	2 hours from the 10:00 interruption	Target validated business service by 12:00.
Observed service recovery	10:00 to 11:45 = 1 hour 45 minutes	Application and business owners confirm usable service.
Maximum tolerable interruption	4 hours for order processing	Business impact analysis establishes the consequence threshold; RTO leaves margin.

Important boundary

A 15-minute replication schedule alone does not prove a 15-minute RPO. Failed checkpoints, replication lag and application inconsistency can increase the real gap. Cyber recovery may also require containment and a clean restore path before systems can return.

03 / CRITICAL ASSETS

Dependencies determine the order.

Sample register excerpt. Each asset has a business function, accountable owner and testable targets.

Asset / function	Owner	RTO / RPO	Dependencies
Identity and DNS - Authentication, naming and emergency access	IT operations	30 minutes / 5 minutes	Independent emergency access; secondary DNS; tested identity recovery
Order application and database - Receive and fulfill customer orders	Operations / application owner	2 hours / 15 minutes	Identity, DNS, network, database replication and recovery-site capacity
Controlled document workspace - Access approved engineering instructions	Engineering / information owner	8 hours / 4 hours	Identity, scoped recovery access, approved storage and data handling
Archive and historical reporting - Historical records and non-urgent reports	Records owner	24 hours / 24 hours	Verified backup copies, keys and catalog

Business impact analysis excerpt

Process	Tolerable interruption	Impact / workaround
Order intake and fulfillment	4 hours	Delayed orders, customer commitments and revenue. Approved manual order log; reconcile before normal service
Engineering document access	1 business day	Delayed engineering and production instructions. Approved controlled offline procedures if permitted; no ad hoc data copies
Historical reporting	2 business days	Deferred management reporting. Defer non-urgent reports

04 / RUNBOOK

Restore usable operations.

Sample actions for the site outage. Acceptance evidence and owner approval are part of each recovery step.

Time	Activity / owner	Acceptance evidence
10:00	Detect primary site outage; open incident record - Incident commander	Record actual outage start; establish a safe communication channel
10:15	Declare recovery; activate manual order intake - Business owner	Confirm customer impact and safe workarounds; preserve transaction log
10:30	Restore identity, DNS and recovery access - IT operations	Validate emergency credentials, least privilege, keys and secondary connectivity
11:00	Promote the validated 09:45 database checkpoint - Database owner	Fence primary writes; verify clean checkpoint and application consistency
11:30	Validate recovery service and reconcile manual orders - Application and business owners	Check record counts, transactions, permissions and external integrations
11:45	Approve resumed order processing - Business owner	Record measured RTO of 1h 45m and recoverable-data gap of 15m; confirm all acceptance checks
Later, after stabilization	Plan and execute controlled return to primary - Change owner	Approve reverse replication, data reconciliation, cutover, rollback and monitoring

05 / EXERCISE REPORT

Measure. Record. Improve.

Fictional exercise findings show how a plan becomes an accountable improvement program.

Test	Observation / metric	Result / follow-up
EX-01 Site outage	Business service resumed at 11:45 after 10:00 interruption. 1h 45m observed vs 2h target	Pass in fictional exercise. Business owner: Retain validation checklist and timestamps
EX-02 Data recovery	Last usable order checkpoint 09:45. 15m gap vs 15m target	Pass in fictional exercise. Database owner: Document reconciliation of uncommitted transactions
EX-03 Dependency check	Emergency identity restored by 10:30. 30m target	Pass in fictional exercise. IT operations: Retest credentials and secondary DNS quarterly
EX-04 Cyber recovery tabletop	Standby checkpoints assumed corrupted; daily isolated copy only. Up to 24h loss vs 15m target	Gap identified. Security and application owners: Evaluate protected checkpoint frequency and clean restore path; agree residual risk
EX-05 Failback review	Return to primary not executed during this example. Test required	Open action. Change owner: Schedule reconciliation, reverse replication and controlled failback exercise

Suggested acceptance evidence

Timestamped incident log; checkpoint and integrity checks; successful test transactions; access validation; manual-order reconciliation; business-owner approval; exercise actions with owners and agreed due dates.

Tailor the next step

Agree critical business processes, outage assumptions, dependencies and recovery acceptance criteria before selecting technology or promising recovery times.