

Backup and continuity

Know what you can recover.

Connect backup scope with the business services that matter, then rehearse recovery. Treat usable restored data, authorized recovery access and cleanup as evidence, alongside the job status.

GOOD FIT Organizations that depend on shared files, cloud data or critical applications and need confidence in their recovery process.

Scope

Recovery priorities - Identify critical workloads, owners and business recovery objectives. Map data, identity, platform and supplier dependencies.

Backup coverage - Review what is protected, where it is retained, administrative separation and failure handling. Make exceptions visible to the owner.

Controlled restore - Agree a safe destination and test scope. Restore the selected workload, confirm usability and measure the observed result.

Continuity procedure - Document the decision path, authorized recovery access, communications, dependencies and post-restore protection/cleanup.

WHAT YOU RECEIVE

- Critical workload and recovery-priority register
- Backup scope and exception review
- Restore exercise plan and observed evidence
- Recovery ownership and communications procedure
- Corrective actions for gaps

CUSTOMER RESPONSIBILITIES

- Set business recovery objectives and data owners.
- Approve the restore destination and timing.
- Maintain required backup products/storage and access.

ACCEPTANCE CHECKS

- Restored data opens and supports the agreed workflow.
- Observed recovery time/data loss is compared with the target.
- Authorized recovery access works.
- Cleanup and re-protection are verified.

SCOPE BOUNDARIES

- Guaranteed recovery time before an actual test
- Unquoted storage, product licenses or application repair
- Unscoped disaster recovery infrastructure
- Live production failover without a separately approved plan

DELIVERY FLOW

PRIORITIZE / REVIEW / RESTORE / IMPROVE