CLOUDSWITCHED

FREE RESOURCE — CLOUD DISASTER RECOVERY PLANNING TEMPLATE

Cloud Disaster Recovery Planning Template

A practical, audit-ready DR plan built around Azure Site Recovery. Set realistic RTO and RPO targets per system, document your replication configuration, define your failover and failback procedures, and keep a real test schedule so you know your DR plan actually works before you need it.

RTO
RECOVERY TIME OBJECTIVE

RPO
RECOVERY POINT OBJECTIVE

ASR
AZURE SITE RECOVERY ALIGNED

Fillable
TICK & TYPE IN ANY VIEWER

AZURE SITE RECOVERY · RTO · RPO · FAILOVER READY · AUDIT-READY

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive PDF

00

How to use this template

This template covers the six core decisions every cloud disaster recovery plan needs to answer: **how fast must each system come back** (RTO), **how much data can you afford to lose** (RPO), **what is replicating where** in Azure Site Recovery, **how do you fail over**, **how do you fail back**, and **how often will you actually test it**. Fill it in once, then keep it under quarterly review — the value comes from it being current, not pristine.

> **AN UNTESTED DR PLAN IS A HOPE, NOT A PLAN**
>
> The single most common failure mode in real disasters is a DR plan that looked great on paper but had never been executed end-to-end. Section 05 builds a real test calendar — commit to at least one full failover test per Tier 1 system per year, plus a quarterly tabletop, and record the actual measured RTO and RPO against the targets you set in Section 01.

The six DR planning sections

- **01 RTO & RPO Targets** — tier every critical system and commit to a measurable recovery target.
- **02 Azure Site Recovery Configuration** — what is replicating from where to where, with which policy.
- **03 Failover Procedure** — the step-by-step runbook for declaring disaster and switching to the recovery region.
- **04 Failback Procedure** — how to return to the primary region cleanly once it is healthy again.
- **05 DR Testing Schedule** — planned tests, scope per test, measured RTO/RPO and lessons learned.
- **06 Communication Plan** — internal and external contacts called during a real DR event, plus sign-off.

Roles to agree before a real DR event

- **DR Commander** — declares the disaster, owns the call on failover and failback, single accountable decision-maker.
- **Technical Lead** — runs the Azure Site Recovery failover, validates services on the recovery side, drives failback when ready.
- **Communications Lead** — status updates to staff, customers and (where relevant) regulators on a defined cadence.
- **Scribe** — keeps a real-time event log so the post-event review has a factual timeline to work from.

01

RTO & RPO Targets

Every system is in one of four tiers. Pick the tier first, then the recovery targets follow. Be honest — targets that look impressive on paper but cost ten times your DR budget will get quietly missed in a real event.

Reference: standard recovery tiers

TIER	RTO TARGET	RPO TARGET	TYPICAL SYSTEMS
Tier 1 — Mission critical	< 1 hour	< 15 minutes	Payment, ERP, customer-facing apps
Tier 2 — Business critical	< 4 hours	< 1 hour	Email, file server, CRM, line-of-business
Tier 3 — Important	< 24 hours	< 4 hours	Intranet, reporting, internal portals
Tier 4 — Non-critical	< 72 hours	< 24 hours	Archive, dev/test, training

Your per-system targets

List every business-critical system. One row per system. The Business owner is the person who signs off the target — not the IT lead who has to deliver it.

SYSTEM / WORKLOAD	TIER	RTO TARGET	RPO TARGET	BUSINESS OWNE

RTO VS RPO — THE DIFFERENCE MATTERS

RTO = maximum acceptable time to bring a system back. **RPO** = maximum acceptable data loss measured in time. Tight RPO drives replication frequency and storage cost; tight RTO drives standby capacity and failover automation. Tier 1 usually needs both tight — the rest is a cost trade-off.

02

Azure Site Recovery Configuration

Document exactly what is replicating, from where to where, and under which policy. Anyone who needs to recover your environment at 3 a.m. should be able to read this page and act — without logging into Azure to find out.

Shared configuration

Primary region _____

Recovery region _____

Recovery Services vault _____

Recovery plan name _____

Default replication policy _____

Subscription / tenant _____

Per-workload replication register

One row per protected VM, managed disk set, or PaaS workload covered by ASR / Azure Backup. Include the replication frequency (Azure-to-Azure ASR is continuous; Azure Backup uses snapshot frequency).

VM / WORKLOAD	TYPE	SOURCE REGION	TARGET REGION	REPLICATION POLICY	TECH OW

DON'T FORGET THE BITS ASR DOES NOT COVER

Azure Site Recovery replicates VMs and disks. It does **not** automatically cover SaaS data (Microsoft 365 mailboxes, SharePoint, OneDrive, Teams), platform identities (Entra ID), DNS records, or secrets in Key Vault. Make sure those are protected by Azure Backup for M365, soft-delete + recovery for Entra, and an immutable export strategy for Key Vault and DNS — and reflect them as separate rows above.

03

Failover Procedure

The runbook for declaring a disaster and switching to the recovery region. Work top-down; do not skip a step because it “looks fine”. Tick each item as it completes, and have the DR Commander confirm before progressing between phases.

Phase 1 — Declare & prepare

- ☐ **Disaster declared** by DR Commander — time, scope and rationale logged.
- ☐ **DR team assembled** — Technical Lead, Comms Lead and Scribe online in a single bridge.
- ☐ **Initial assessment** confirms primary region is unrecoverable within the declared RTO window.
- ☐ **Stakeholder notification** sent: leadership, affected business owners, customer support.
- ☐ **Latest replication health** verified in the Recovery Services vault — RPO is within target.

Phase 2 — Execute failover

- ☐ **Recovery plan triggered** from the Azure portal (or via PowerShell / runbook automation).
- ☐ **Tier 1 workloads brought up first** in the order defined by the recovery plan.
- ☐ **Network configuration** applied in the recovery region — VNets, NSGs, route tables, peerings.
- ☐ **DNS records updated** — public records (TTL pre-lowered) and internal Private DNS zones swung to recovery endpoints.
- ☐ **VPN / ExpressRoute** recovery circuits brought online; on-prem connectivity restored.
- ☐ **Tier 2 and Tier 3 workloads** failed over in dependency order.

Phase 3 — Validate & commit

- ☐ **Application smoke tests passed** on every Tier 1 system — signed off by the business owner.
- ☐ **Users notified** that service is restored, with any known limitations called out.
- ☐ **Failover committed** in ASR — recovery point selected and locked.
- ☐ **Reverse replication enabled** from recovery region back to (a healthy) primary region.
- ☐ **Failover timeline logged** by the Scribe — actual RTO and RPO captured for the post-event review.

04

Failback Procedure

Failback is the return journey to the primary region once it is healthy again. Treat it as a planned operation in a maintenance window — a controlled failover with the source and target reversed.

Phase 1 — Confirm primary is healthy

- **Root cause resolved** in the primary region — Azure region status green for at least 24 hours.
- **Infrastructure rebuilt** where required — VNets, NSGs, identity, networking peerings reconciled.
- **Reverse replication healthy** — recovery-to-primary replication caught up, lag within RPO target.
- **Failback window agreed** with the business — user notifications scheduled.

Phase 2 — Execute failback

- **Quiesce writes** in the recovery region — freeze applications and confirm replication lag is zero.
- **Recovery plan triggered** back to the primary region with the reverse direction.
- **Tier-ordered restart** in primary — Tier 1 first, then Tier 2, Tier 3 in dependency order.
- **DNS records restored** — public + Private DNS swung back to primary endpoints (TTLs lowered first).
- **Network paths restored** — VPN / ExpressRoute back to primary, recovery-region paths quiesced.

Phase 3 — Validate & re-protect

- **Smoke tests passed** on every Tier 1 system in the primary region — business owner sign-off captured.
- **Replication re-enabled** from primary back to recovery region — ASR back into normal protection direction.
- **Backup jobs resumed** in the primary region and verified on the next scheduled run.
- **Users notified** service is fully restored, with the DR event timeline summary attached.
- **Post-event review** scheduled within five business days — calendar invite issued to all responders.

05

DR Testing Schedule

The single best predictor of recovering successfully in a real disaster is how often you have practiced. Pick a cadence per test type and stick to it — then record actual measured RTO and RPO against the Section 01 targets.

Reference: minimum recommended cadence

TEST TYPE	CADENCE	WHAT IT PROVES
Tabletop walkthrough	Quarterly	Runbook still reads correctly, team knows their roles
ASR Test Failover (non-disruptive)	Quarterly per Tier 1	Recovery point boots and applications start in the test network
Live failover (single workload)	Annually per Tier 1	Real failover and failback against measured RTO / RPO
Full DR exercise (multi-tier)	Annually	End-to-end recovery including comms, DNS and dependencies

Test calendar & results

One row per test executed. Capture the measured outcome — not the planned one.

DATE	TEST TYPE	SCOPE & SCENARIO	RTO MEASURED	RPO MEASURED	PAS FAI

06

Communication Plan & Sign-off

In a real DR event you do not have time to look up phone numbers — capture every contact you might need now. The internal table is your DR team; the external table is everyone outside the company you may need to call.

Internal DR contacts

ROLE	NAME	PHONE	EMAIL	BACKUP CONTACT
DR Commander				
Technical Lead				
Communications Lead				
Scribe				
Executive sponsor				

External contacts

PARTY	CONTACT / ACCOUNT	PHONE	EMAIL / PORTAL
Microsoft Azure support			
Internet / ISP			
Cyber insurance			
Key vendor / SaaS			
ICO (if data breach)	0303 123 1113	0303 123 1113	ico.org.uk/report-breach

PREPARED BY _____ **DATE** _____ **APPROVED BY** _____

CLOUDSWITCHED

CLOUD BACKUP & DISASTER RECOVERY

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom