

Disaster Recovery Plan Template

A free, adaptable template covering recovery tiers with RTO and RPO, failover strategy, a numbered runbook, testing, and SOC 2 / ISO 27001 / HIPAA / GDPR alignment.

Company: _____

Effective date: _____

Plan owner: _____

Review cycle: Annually, after any major architecture change, and after every real disaster

HOW TO USE THIS TEMPLATE

Replace every bracketed placeholder with your organization's specifics. Example RTO and RPO values are illustrative starting points, not benchmarks: measure your real restore times and set your own. Route the finished plan through your normal approval process. This template is a starting point, not legal advice. See ComplyJet's [Disaster Recovery Plan Template guide](#) for the reasoning behind each section.

1. Purpose and Scope

This plan defines how [Company Name] restores IT systems and data after a disaster: an outage, data loss event, or loss of a data center or cloud region. It applies to all in-scope production systems listed in Section 2. It covers systems recovery only. Business-wide continuity (business impact analysis, workforce relocation, manual workarounds) is covered in [Company Name]'s Business Continuity Plan, and security-incident handling in the Incident Response Plan.

2. System Inventory

System	Owner	Dependencies	Recovery tier	Last restore test
[Production application]	[Name]	[DB, auth, DNS]	[1]	[Date]
[Primary database]	[Name]	[Storage, KMS]	[1]	[Date]
[Internal tools]	[Name]	[SSO]	[2]	[Date]
[Add rows]				

3. Recovery Tiers, RTO, and RPO

RTO (recovery time objective) is the maximum time a system can be down. **RPO** (recovery point objective) is the maximum data loss, measured in time. Each system owner signs off on the tier for their system.

Tier	Example systems	Example RTO	Example RPO	Your RTO / RPO	Measured restore time
1: Critical	Production app, primary database, authentication	1 hour	5 minutes	[] / []	[]
2: Important	Admin tools, job queues, billing sync	4 hours	1 hour	[] / []	[]
3: Standard	Analytics, wiki, ticketing	24 hours	24 hours	[] / []	[]
4: Low	Dev sandboxes, archived reports	72 hours	1 week	[] / []	[]

WATCH OUT

A target nobody has measured is a wish. If your RTO is one hour and your last restore took five, the plan is wrong, not optimistic.

4. Failover Strategy Selector

Choose one strategy per tier. Strategies follow the four options in AWS's Disaster Recovery of Workloads whitepaper; the same logic applies on other clouds and physical sites.

Strategy	How it works	Speed	Cost	Used for tier
Backup and restore	Rebuild from backups after a disaster	Slowest	Lowest	[]
Pilot light	Core pieces (e.g. database) in standby; rest switched on in a disaster	Faster	Low to moderate	[]
Warm standby	Scaled-down full copy with live replicated data	Fast	Moderate to high	[]
Multi-site active/active	Full second production environment serving traffic	Near-instant	Highest	[]

Secondary site / region: [Name and location]. Backup locations and retention: [Details]. Backups are encrypted and stored separately from the primary environment.

5. Roles and Activation Authority

Role	Responsibility	Primary	Backup
Activation authority	Declares and stands down the disaster	[Name]	[Name]
Recovery lead	Runs the runbook and coordinates technical recovery	[Name]	[Name]
Communications lead	Internal updates, customer notices, status page	[Name]	[Name]
System owners	Restore and verify their own systems	[Names]	[Names]

Contact list location (stored outside the environments being recovered): [Location].

6. Declaration Criteria

A disaster is declared when any of the following is true: a Tier 1 system is expected to be unavailable for longer than [30 minutes]; data loss beyond the stated RPO is confirmed; the primary site or region is lost; [add your own].

7. Recovery Runbook

#	Step	Owner	Time box
1	Assess and declare. Confirm the event matches a declaration criterion; activation authority declares and logs the time.	Activation authority	[]
2	Assemble the team. Notify the recovery team and backups; open a dedicated incident channel.	Recovery lead	[15 min]
3	Communicate. First internal and customer update; follow the update cadence.	Communications lead	[]
4	Fail over in tier order. Tier 1 first, then Tier 2 and below, per each tier's strategy.	Recovery lead	Per RTO
5	Verify. Data integrity against RPO, core user journeys, authentication, integrations.	System owners	[]
6	Run in recovery mode. Monitor closely; hold risky deploys.	Recovery lead	[]
7	Fail back. Move traffic back in a planned window after reconciling data.	Recovery lead	[]
8	Review. Post-recovery review within [5] business days; update this plan.	Plan owner	[]

8. Communication Plan

Audience	Channel	First update within	Cadence	Owner
Internal staff	[Slack / email]	[30 min]	[Hourly]	Communications lead
Customers	[Status page / email]	[1 hour]	[Every 2 hours]	Communications lead
Regulators / auditors (if required)	[Per framework]	[Per framework]	[]	[Legal / Compliance]

9. Testing Schedule and Log

Test	What it catches	Suggested cadence
Tabletop walkthrough	Unclear roles, missing contacts, gaps in declaration criteria	At least annually and after team changes
Backup restore test	Corrupt backups, stale credentials, undocumented steps	Quarterly for Tier 1; at least annually for the rest
Failover test	Broken replication, capacity limits, DNS and config surprises	At least annually for Tier 1

Cadences are recommendations, not values prescribed by any framework. Record each test below.

Date	Test type	Scenario	Measured recovery time vs RTO	Fixes and owner
[]	[]	[]	[]	[]
[]	[]	[]	[]	[]

10. Framework Alignment

Framework	Where it lives	What it expects
SOC 2	Availability category, A1.2 and A1.3	Backup processes and recovery infrastructure in place; recovery plan procedures tested. Applies when Availability is in audit scope.
ISO 27001:2022	Annex A 5.30, with 8.13 and 8.14	ICT continuity planned, implemented, maintained, and tested against business continuity objectives.
HIPAA	45 CFR 164.308(a) (7)	Data backup plan, disaster recovery plan, and emergency mode operation plan required; testing and revision, and criticality analysis, are addressable.

GDPR	Article 32(1)(c)	Ability to restore availability of and access to personal data in a timely manner after an incident.
------	------------------	--

This is a starting reference, not a substitute for reading each framework's current text.

11. Sample Clauses

CLAUSE 3.1: RECOVERY OBJECTIVES

Every in-scope system is assigned to a recovery tier by its system owner. Tier 1 systems have a recovery time objective of [1 hour] and a recovery point objective of [5 minutes]. Tier assignments and objectives are reviewed annually and after any major architecture change. The most recent measured restore time for each Tier 1 system is recorded in the recovery register.

CLAUSE 6.1: DECLARING A DISASTER

[Role, e.g. CTO] is the activation authority, with [named backup] as alternate. A disaster is declared when a Tier 1 system is expected to be unavailable for longer than [30 minutes] or when data loss beyond the stated recovery point is confirmed. The declaring party logs the time of declaration and notifies the recovery team within 15 minutes.

Produced by ComplyJet as a free companion to the [Disaster Recovery Plan Template](#) guide. ComplyJet helps SaaS startups turn plans like this one into evidence-backed controls across SOC 1, SOC 2, ISO 27001, HIPAA, GDPR, PCI DSS, and 25+ other frameworks. [Book a free demo](#) to see how.