MR.PLANB FIELD GUIDE · BACKUP AND DR

Disaster Recovery Plan: Template and Checklist Pack

How to turn backups into a recovery process another person can execute, with tiers, roles, a Proxmox sequence and a test schedule.

Updated **2026-10-29** · Full guide: www.mrplanb.com/storage/disaster-recovery-plan

> A backup tells you where the data is. A disaster recovery plan tells you what to do next: who has authority, which copy to use, and in what order. A good plan sets RPO and RTO per workload, maps dependencies, names roles, protects recovery credentials and is tested regularly.

34 items in the plan checklist

4 recovery tiers, from foundational to deferrable

8 named roles in the response

10 sections in a complete plan document

Backup vs disaster recovery

	Backup	Disaster recovery
Does	Creates recoverable copies of data	Restores complete services after disruption
Focus	Protection and retention	Recovery sequence and operation
Answers	Where the data is stored	How the service will return
Automation	Can be largely automated	Needs technical and organizational decisions
Communication	Not defined	Roles, escalation, status reporting

Recovery tiers

Tiers should reflect dependencies as well as business importance. A low-visibility DNS or identity server may need to recover first.

Tier	Examples
Tier 0, Foundational	Identity, DNS, network management, core storage, backup infrastructure, secrets
Tier 1, Critical production	Transaction databases, customer applications, payment systems, production APIs
Tier 2, Important internal	File servers, collaboration tools, internal applications, monitoring
Tier 3, Deferrable	Development, test, historical reporting, nonessential archives

Choosing a recovery strategy

Match the strategy to the workload's RPO, RTO, risk and budget.

Strategy	Best suited to
Backup and restore	Longer RTO, lower cost, systems that tolerate rebuilding
Pilot light	Moderate RTO, applications that can be automated
Warm standby	Shorter RTO, important customer services
Active-active / multi-site	Very short recovery targets, workloads that justify the cost

Proxmox recovery order

A suggested sequence for three Proxmox VE nodes, a local PBS, a remote backup copy and typical VMs.

1. Network and firewall access
2. Recovery credentials
3. Replacement Proxmox host or cluster
4. Backup repository access
5. Identity and DNS
6. Database
7. Business application
8. File server
9. Monitoring
10. Development systems

Testing schedule

Activity	Suggested frequency
Review contacts and ownership	Quarterly
Review recovery documentation	Quarterly
Verify backup and replication status	Daily or weekly
Restore selected files	Monthly
Restore a complete system	Monthly or quarterly
Test access to offsite backups	Quarterly
Run a tabletop exercise	Twice yearly
Run a broad DR exercise	Annually
Review after major changes or an incident	Every time

The ten sections of a plan

- [ ] Document control
- [ ] Purpose and scope
- [ ] Activation criteria

- [ ] Recovery objectives (RPO and RTO)
- [ ] System inventory
- [ ] Dependency map
- [ ] Recovery strategy
- [ ] Roles and contacts
- [ ] Recovery procedures
- [ ] Testing and maintenance

Sources and notes: NIST contingency planning and disaster recovery plan definition · AWS guidance on RPO, RTO and recovery strategies · CISA ransomware recovery guidance