CONTINUITY HUB • QUICK FIELD REFERENCE

DR Plan Quick Card: Disaster Recovery Planning Field Reference

OPERATIONAL DR FIELD CARD • FREE RUNG
Current version — Nov 2, 2026. Update history: https://continuityhub.org/disaster-recovery-planning-complete-professional-guide/

1. WHAT A DISASTER RECOVERY PLAN IS (SCOPE & PURPOSE)

OPERATIONAL SCOPE

A **disaster recovery (DR) plan** establishes how technology services are reconstituted after a disruption. It names the systems, the return order, recovery time (RTO), recovery point (RPO), and the roles empowered to declare failover. It is narrower than the business continuity plan (BCP), which covers enterprise-wide survival (workforce safety, customer comms, supply chain, manual workarounds). Disaster recovery strictly powers the technical infrastructure: data centers, cloud environments, virtualized workloads, relational/distributed databases, telecommunications, and application middleware.

2. START FROM THE IMPACT, NOT THE TOOL (BIA GROUNDING)

RISK ANALYSIS

Recovery priorities derive strictly from the Business Impact Analysis (BIA)—never buy a hot site because a vendor slide shows one. Inverting risk posture (e.g. active-active clustering for internal reporting while payment portals sit on nightly backups) wastes IT capital. Every tier must be justified by quantifiable downtime consequences:

Direct Financial Loss: Lost sales volume, transactional revenue leakage, and contractual SLA penalty payouts.

Regulatory & Fiduciary Impact: Mandatory disclosure rules: SEC 4-day disclosure windows, DORA 4-hour initial incident filings, FFIEC 36-hour notifications, and statutory penalties.

Cascading Operational Failure: Upstream core outages paralyzing downstream workflows, physical logistics, or customer support centers.

3. THE RTO AND RPO TIER HIERARCHY

TECHNICAL TARGETS

RTO (Recovery Time Objective): Maximum acceptable duration of system unavailability. • **RPO (Recovery Point Objective):** Maximum acceptable data loss measured in transaction time.

Tier Classification	Target RTO	Target RPO	Target Architectural Posture
Tier 0: Mission Critical	< 15 – 30 minutes	near-zero data loss target	Active-active multi-region clustering, synchronous data replication, automated health checks with traffic failover.
Tier 1: Business Critical	< 2 – 4 hours	< 15 minutes	Warm standby replica instances, continuous asynchronous replication, pre-scripted container orchestration spin-up.
Tier 2: Core Operational	< 12 – 24 hours	< 4 hours	Automated cloud infrastructure-as-code (Terraform/Ansible) provisioning, point-in-time snapshot restoration from remote cloud vaults.
Tier 3: Administrative	> 48 – 72 hours	< 24 hours	Cold standby or bare-metal reinstall, periodic object archive restore, manual workstation reprovisioning.

4. THE RECOVERY CHOICES (FACILITY & CLOUD POSTURES)

ARCHITECTURE MENU

Recovery Posture	Operational Characteristics & Recovery Reality
Cold Site	Basic facility space and power or bare-metal hardware; data restored from archive; slowest and lowest-cost posture.
Warm Site	Equipment ready and data copied on a scheduled asynchronous basis; typically reconstituting services within hours.
Hot Standby	Live capacity provisioned with continuous synchronous/near-synchronous replication; automated cutover within minutes.
Cloud & DRaaS	Elastic cloud infrastructure capable of implementing cold, warm, or hot postures dynamically with software-defined networking.

Plan Mandate: The plan must explicitly record which posture each service uses and where the primary and secondary copies of data reside.

5. MODERN BACKUP ARCHITECTURE: THE 3-2-1-1-0 IMMUTABLE RULE

RANSOMWARE DEFENSE

- **3 Copies of Data:** Maintain at least three independent copies of all critical production data (1 primary production copy and 2 distinct backup sets).
- **2 Different Media Types:** Store data across at least two distinct storage technologies (e.g. enterprise SAN flash block storage and cloud object storage).
- **1 Copy Stored Offsite:** Maintain at least one backup copy in a physically separated alternate cloud region or geographically remote data center outside hazard zone.
- **1 Copy Immutable / Air-Gapped:** Protect at least one copy with write-once-read-many (WORM) storage with strict Object Lock compliance policies, or isolate in an out-of-band, air-gapped recovery vault in a separate account with separate credentials.
- **0 Backup Restoration Errors:** Verify zero unrecoverable errors through automated daily checksum validations and recurring end-to-end sandbox restoration testing.

CONTINUITY HUB • QUICK FIELD REFERENCE

DR Plan Quick Card: Runbooks, Stranger Test, Testing Continuum & Governance

OPERATIONAL DR FIELD CARD • FREE RUNG
Current version — Nov 2, 2026. Update history: https://continuityhub.org/disaster-recovery-planning-complete-professional-guide/

6. THE STRANGER TEST: "WRITE THE PLAN SO SOMEONE ELSE CAN RUN IT"

3:00 AM STANDARD

The Core Stranger Test: A plan that only the author can execute is not a plan. Runbooks must be written for the engineer on call at 3:00 AM under conditions of high stress, imperfect information, and severe operational pressure. If recovery relies on undocumented tribal folklore or institutional memory possessed solely by the primary architect, failover will collapse during a catastrophic event.

7. ESSENTIAL RUNBOOK COMPONENTS & DETERMINISTIC 5-STEP SEQUENCING

TECHNICAL EXECUTION

1. Explicit Declaration Authority: Name specific role titles (CIO, VP Engineering, DR Incident Commander). Define objective thresholds (e.g. uncontained database corruption > 30 min approaching RTO).
2. Out-of-Band Comms & Secure Access: Pre-authenticated channels independent of disrupted corporate SSO/Slack/email (dedicated secure Signal groups, secondary cloud tenants, hard-copy hardware vaults).
4. The Failback Protocol: Reverse resynchronization workflows from secondary site back to repaired primary, transaction reconciliation procedures, and scheduled maintenance windows for reverse cutover.
Supply Chain Incident Coordination: Tight alignment with supply chain disruption response when facilities or logistics are impaired.

3. Deterministic Step-by-Step Technical Sequencing (Copy-Paste Chronological Order):

1. **Step 1 – Traffic Quiescence:** Divert incoming production traffic or place applications into maintenance mode to halt transactional writes.
2. **Step 2 – Data Replication Verification:** Validate replication catch-up logs, confirm replica consistency, and break replication pairing to promote secondary database to primary.
3. **Step 3 – Infrastructure Provisioning:** Spin up container clusters or compute virtual machines via automated infrastructure-as-code (Terraform/Ansible) manifests.
4. **Step 4 – Network and DNS Routing Cutover:** Update global server load balancers (GSLB) or modify external DNS A/CNAME records with pre-reduced Time-to-Live (TTL) values.
5. **Step 5 – Automated Health Checks & Validation:** Execute automated synthetic transaction tests before reopening traffic gates to external users.

8. TEST BEFORE YOU NEED IT: THE 3-LEVEL VALIDATION CONTINUUM

EXERCISE CADENCE

The Testing Law: A recovery that has not been run is a hypothesis. Testing confirms recovery time (RTO) and recovery point (RPO) against the last copy, not against the architecture diagram. *Never file a test as a pass if users could not actually work.* Record the gap and fix the plan.

Validation Exercise	Cadence	Scope, Execution Method & Deficiencies Uncovered
1. Tabletop Walkthrough	Semi-Annual	Structured seminar with technical leads, app owners, incident commanders. Validates role assignments, decision escalation, and procedural ambiguities before touching systems.
2. Functional & Simulation	Annual	Technical execution in isolated sandbox/staging without live traffic. Restores from immutable cloud snapshots, spins clusters via automation scripts. Measures real duration vs RTO; uncovers storage throughput bottlenecks, missing env vars, expired SSL/TLS certificates.
3. Full-Scale Chaos Drills	Annual (Tier 0)	Controlled maintenance windows. Intentionally terminates primary regions, severs replication, executes chaos engineering (Chaos Mesh, AWS Fault Injection Simulator). Formally logs gaps in After-Action Reports (AAR) with assigned remediation milestones.

9. KEEP THE PLAN CURRENT: 4 CONTINUOUS GOVERNANCE TRIGGERS

PLAN MAINTENANCE

Change the plan when a system, provider, or recovery target changes. An unchanged plan after a cloud migration describes a data center you no longer have:

1. Architecture & Cloud Migration: Transitions from on-prem DBs to managed cloud clusters, monoliths to Kubernetes, or new SaaS adoptions mandate immediate runbook revisions.

2. Post-Incident & Exercise Remediation: Deficiencies uncovered during routine outages or exercises mapped to Corrective Action Plans (CAPs) with strict 30-day deadlines.

3. Scheduled Recertification: Business application owners and lead architects formally review and recertify runbooks on a strict annual cycle.

4. Continuous Automated Verification: CI/CD pipeline checks continuously verify new infrastructure adheres to backup tags, replication monitoring, and immutable vaults.