BRISKDATA ENGINEERING TEMPLATE | DOC ID: BD-OPS-DR-001 | ADAPTABLE TEMPLATE

Disaster Recovery Runbook Template

System-Level Failover, Isolated Restore, Split-Brain Fencing, and Recovery Timing Verification

SCOPE AND CLOCK DEFINITION

Use one copy of this technical runbook per critical system. Store an offline copy accessible when primary SSO or internal wikis are unavailable. Measure observed RTO from the start of service disruption until business verification and traffic restoration complete, recording detection and authorization intervals separately.

1. System Identification and Recovery Objectives

Parameter	System Specification (Replace Placeholders)	Owner / Verification
System / Workload Name	[e.g., Core Customer Portal & Primary Relational Database]	[Service Owner]
Criticality Tier	[e.g., Tier 1 - Customer Transaction / Operations Critical]	[Per IT DRP BD-GOV-DRP-005]
Target RTO (Disruption to Restored)	[e.g., 2 hours total wall-clock from disruption start]	[Tested cadence, e.g., Quarterly]
Target RPO (Max Data Loss)	[e.g., 15 minutes via continuous log archival]	[Backup / Replica monitor]
Primary Environment	[Cloud Region / Data Center / Account / VPC or Subnet ID]	[Infrastructure Lead]
Recovery Environment	[Secondary Region / Isolated Recovery VPC / Standby Host]	[Infrastructure Lead]
Out-of-Band Access & Keys	[Emergency Vault Location, Break-Glass Role, KMS/Encryption Keys]	[IC + On-Call Lead]

2. Preconditions, Declaration Authority, and Isolation Rules

- **Declaration Authority:** Confirm recovery activation with [Authorized Role, e.g., Incident Commander + CTO/Ops Director] before promoting a standby database or changing authoritative DNS for live traffic.
- **Split-Brain Write Fencing:** During a live failover, block writes to the degraded primary environment (load balancer maintenance rule, security group, or connection revoke) before promoting a replica so diverging writes cannot occur.
- **Isolated Drill Side-Effect Controls:** When running a scheduled recovery test in a fenced network, disable outbound SMTP, payment processor captures, SMS/webhook dispatch, and production cron jobs before starting application workers.

3. Ordered Recovery and Cutover Sequence

Step	Phase	Recovery Action (Adapt Commands to Workload)	Owner	Expected Verification	UTC Time
01	Declare & Fence	[Open incident bridge, confirm authority, and fence primary writes if live failover]	[IC / Net]	[Primary writes halted or drill VPC isolated]	[HH:MM]
02	Data Recovery	[Promote cross-region replica OR restore immutable backup to target recovery point]	[DB Lead]	[Database online; inspect last committed timestamp]	[HH:MM]

Step	Phase	Recovery Action (Adapt Commands to Workload)	Owner	Expected Verification	UTC Time
03	Secrets & Config	[Point recovery compute environment to restored database and disable external side effects if drill]	[SRE / App]	[Config validated; external webhooks safe]	[HH:MM]
04	Compute Scale-Up	[Start / scale application services and background workers in recovery environment]	[SRE / App]	[Health probes return 200 OK across nodes]	[HH:MM]
05	Business Checks	[Execute authentication, representative read/write workflow, and data integrity queries]	[Tech Lead]	[Workflows pass; row counts/balances verified]	[HH:MM]
06	Traffic Cutover	[Live event only: update DNS / load balancer origin pool and monitor error rates]	[Net / SRE]	[External traffic healthy for 30+ minutes]	[HH:MM]

ILLUSTRATIVE POSTGRESQL REPLICA LAG & RESTORE VERIFICATION QUERIES (ADAPT TO YOUR ENGINE)

```
# Check replication replay lag and last received WAL location before promoting a PostgreSQL replica
psql "host=<RECOVERY_DB_HOST> user=<DR_ADMIN> dbname=<DB_NAME>" \
  -c "SELECT now() - pg_last_xact_replay_timestamp() AS lag, pg_last_wal_receive_lsn(),
pg_last_wal_replay_lsn();"

# Verify latest committed business timestamp after restore to calculate observed RPO
psql "host=<RECOVERY_DB_HOST> user=<DR_ADMIN> dbname=<DB_NAME>" \
  -c "SELECT max(created_at) AS latest_record_utc, count(*) AS total_rows FROM <CRITICAL_TABLE>;"
```

4. Recovery Timing Log and Post-Recovery Checklist

Timing Milestone	Recorded UTC Timestamp	Notes / Evidence Link
1. Service Disruption Began (T0)	[YYYY-MM-DD HH:MM:SS UTC]	[Alert / telemetry source]
2. Incident Detected & Recovery Authorized	[Detected UTC] | [Authorized UTC]	[Detection + decision elapsed minutes]
3. Data Store Restored & Verified	[YYYY-MM-DD HH:MM:SS UTC]	[Last recovered commit timestamp -> Observed RPO]
4. Business Verification & Traffic Restored	[YYYY-MM-DD HH:MM:SS UTC]	[Milestone 4 minus Milestone 1 -> Observed RTO]

- [ ] **Reconcile Deferred Transactions:** Review queued webhooks, batch files, or manual fallback records accumulated during the outage.
- [ ] **Plan Controlled Failback:** Re-establish standby replication and schedule failback during an approved maintenance window.
- [ ] **Archive Drill / Recovery Evidence:** Save timing logs, verification screenshots, and gap tickets to [Compliance / Ops Evidence Folder].

Template Reuse Note: You may copy and adapt this template for internal operations within your organization. Replace bracketed placeholders and remove example entries before adoption. briskData branding and third-party trademarks remain the property of their respective owners.