1. EXERCISE IDENTIFICATION & BOUNDED SCOPE

Exercise Name	.....	**Date / Window**	.....
Simulated Scenario	..... (e.g., Primary data center complete power loss at 9:15 AM; ransomware isolation; cloud storage region failure)		
Scope IN (Included Systems, Sites & Teams)			
Scope OUT (Explicit Exclusions)	State explicitly which databases, environments, integrations, and user groups are NOT touched.		

2. OBJECTIVES STATED AS VERIFIABLE CLAIMS

Rule: Formulate objectives as claims to be proven on paper, not general activity descriptions. Pre-set exact success criteria.

#	Verifiable Claim (e.g., "The order database is serving transactions within its RTO")	Pre-Set Success Criteria (Decided in Advance)
C1	.....	.....
C2	.....	.....
C3	.....	.....

3. ROLES, AUTHORITY & PRODUCTION SAFEGUARDS

Role	Assigned Individual(s)	Test Day Responsibilities
Test Director / Facilitator	.....	Runs to plan, controls scenario/injects, owns the master clock.
Recovery Performers	.....	Execute procedures strictly from written runbooks.
Observers & Evaluators	.....	Record timeline, deviations, stalls, and functional verifications.
System / App Owners	.....	Validate restored data wholeness and application functionality.
Decision-Maker / Risk Owner	.....	Named leader authorized to proceed, escalate, or abort.
Named STOP Authority	.....	**Holds explicit authority to abort test if safeguards are breached.**

Production Safeguards & Rollback Script: Document the exact technical isolation mechanisms (isolated network VLANs, snapshot branches, sandboxed DNS) and step-by-step rollback procedures. If the test threatens production operations or breaches scope, STOP authority triggers immediate abort.

1. PRE-EXECUTION FIDELITY VERIFICATION

Execution Rule: The people who perform recovery in an incident must perform it in the test from the written procedures — not from unwritten memory. If the expert must go off-script to succeed, the plan has a defect even if recovery worked. "*A test the hero saves is a test the plan failed.*"

Sign	Run-From-The-Document Rule Check	Verification Notes & Status
[ ]	All recovery steps are executed from current, written procedures.	.....
[ ]	Command syntax is copied/run from the runbook (not remembered).	.....
[ ]	Credentials and access tokens are pulled from documented vaults.	.....
[ ]	Dependencies are engaged in the documented sequence.	.....
[ ]	Any off-script action is halted and immediately logged below.	.....

2. DEVIATION & IMPROVISATION LOG (PLAN DEFECTS)

Log every instance where an engineer diverged from written steps, bypassed a documented command, or called unlisted personnel.

Time	Step # / Runbook	Observed Deviation / Improvisation	Root Cause (Stale Doc / Dependency)	Doc Fix Required
.....	.....	.....	.....	.....
.....	.....	.....	.....	.....
.....	.....	.....	.....	.....
.....	.....	.....	.....	.....

3. PROCEDURE FIDELITY EVALUATION SUMMARY

Total Documented Steps Executed	.....	**Total Unscripted Deviations**	.....
Did Recovery Rely on Hero Improvisation?	[ ] **NO** — Executed cleanly from documentation [ ] **YES** — Plan defective; documentation update required prior to re-test		

1. RTO RECOVERY STOPWATCH (DECLARED FAILURE TO USABLE SERVICE)

The clock runs from declared failure to demonstrably usable service — not when green lights appear.

Timeline Milestone	Exact Timestamp	Elapsed Time	Observer Notes & Verification Point
T0: Simulated Failure Injected	.....	00:00	Scenario event started by Test Director
T1: Failure Detected	.....	.....	Alert fired by monitoring system
T2: Outage Declared / Decision	.....	.....	Decision made vs "is it really down?" stall
T3: Technical Recovery Complete	.....	.....	Data restored / infrastructure online
T4: Verified Service Usable	.....	.....	Business users transact successfully
Total Measured Recovery Time	**T4 − T0 =**		**Accepted RTO:** .....
RTO Finding Status	[ ] **BEAT OBJECTIVE** [ ] **MET OBJECTIVE** [ ] **MISSED OBJECTIVE (GAP FINDING)**		

2. RPO DATA POSITION AUDIT

Accepted RPO Limit (from BIA)	.....	**Failure Declaration Time**	.....
Timestamp of Newest Restored Data	.....	**Measured Data Loss Lag**	.....
RPO Finding Status	[ ] **INSIDE RPO** — Restored data lag meets business criteria. [ ] **EXCEEDED RPO (DEFECT)** — Restored data older than agreed limit; replication/backup failed.		

3. APPLICATION FUNCTIONAL VERIFICATION CHECKLIST

Functional Check	User Group / Evaluator	Pass / Fail	Specific Defect or Failure Details
User Authentication & Directory Login	.....	[ ] Pass [ ] Fail	.....
Core Transaction Processing (Write)	.....	[ ] Pass [ ] Fail	.....
Reporting & Query Functions (Read)	.....	[ ] Pass [ ] Fail	.....
Integration Feeds / External APIs	.....	[ ] Pass [ ] Fail	.....

1. THE 4-POINT RESTORATION VERIFICATION SHEET

Backup success reports only prove data was written. Only a restore proves it can be read back into a working system.

Pt	Verification Standard	Inspection Criteria	Status	Sign-Off
1	**Readable & Restorable**	Media accessible; file archive uncorrupted; decryption succeeds; data mounts in isolated target.	[ ] PASS [ ] FAIL	.....
2	**Inside RPO**	Timestamp of newest data record lags failure time by less than the accepted RPO limit.	[ ] PASS [ ] FAIL	.....
3	**Data Wholeness**	Record counts match source logs; table integrity checks pass; application-level schemas validate.	[ ] PASS [ ] FAIL	.....
4	**System Actually Starts**	Application daemon starts, dependencies bind, SSL certificates valid, host licenses recognized.	[ ] PASS [ ] FAIL	.....

2. THE ROTATE BACKUPS RULE & TIMING FLOOR SHEET

Rotation Rule: Testing the same convenient backup proves only that backup. Maintain a rotating schedule of target databases, snapshot dates, and backup sets. The duration of restore is the absolute floor of recovery time.

Test Date	Backup Set / Snapshot ID	Data Date	Restore Duration	System Started?	Floor Recorded
.....	.....	.....	.....	[ ] Y [ ] N	.....
.....	.....	.....	.....	[ ] Y [ ] N	.....
.....	.....	.....	.....	[ ] Y [ ] N	.....

Restoration Floor Warning: If technical restore duration alone exceeds or consumes more than 70% of the RTO, the objective cannot be met once detection, decision, and verification are added. Escalate immediately for engineering redesign.

1. FAILOVER SEQUENCE CHECKLIST

Sequence Phase	Mandatory Action & Procedure Verification	Observed Metric	Pass / Fail
1. Declare Failure	Inject simulated primary outage per scenario specification.	Inject:	[ ] Done
2. Detect & Decide	Monitor alert time; track decision vs "is it really down?" stall.	Stall: ..... min	[ ] Done
3. Switch Execution	Initiate automated or manual failover; switch traffic/routing.	Duration:	[ ] Done
4. Function Verify	Business users exercise authentic transactional workflows.	Checks passed:	[ ] Done
5. RPO Position	Verify data currency and measure transaction lag.	Lag: ..... min	[ ] Done
6. Deliberate Failback	Execute documented return procedure with data reconciliation.	Reconciled:	[ ] Done

2. DELIBERATE FAILBACK RECONCILIATION PROTOCOL

Returning to primary is an independent procedure with its own data risks. More than one organization has survived failover and injured itself on the return.

Failback Stage	Verification Action	Status
Delta Data Capture	Isolate and capture all new transactions written to the recovery site during the test window.	[ ] Reconciled
Reverse Synchronization	Synchronize delta data back to the primary database before redirecting active user traffic.	[ ] Reconciled
Reconciliation Validation	Verify transaction sequence numbers and database consistency checksums match across both sites.	[ ] Verified

3. PARALLEL TEST DISCIPLINE & CUTOVER LIMITS

Data Discipline Protocol (Strict Isolation)	Cutover Limit Acknowledgment
• Recovery systems run strictly on isolated snapshot copies. • **Production data is NEVER written by the test.** • Outbound notification services disabled or redirected to test sink. • Compare parallel workload outputs with live production output.	• A parallel test proves capacity under load, but **does NOT prove cutover**. • DNS resolution changes are unexercised. • Connection string switches are unexercised. • Pair with a separate, safeguarded cutover test.