PRINTABLE & FILLABLE WORKBOOK • $7 TIER
Current version — Nov 2, 2026. Update history: https://continuityhub.org/disaster-recovery-planning-complete-professional-guide/

SHEET 1: BUSINESS IMPACT ANALYSIS (BIA) & TIER ASSIGNMENT WORKSHEET

START FROM IMPACT

Core Principle: Start from the impact, not the tool. Never select a hot site because a vendor slide shows one. Every tier assignment must be justified by quantifiable downtime consequences across three dimensions: **(1) Direct Financial Loss** (lost sales, transactional leakage, SLA penalties); **(2) Regulatory & Fiduciary Impact** (SEC 4-day disclosure, DORA 4-hour initial filing, FFIEC 36-hour notification, statutory fines); **(3) Cascading Operational Failure** (upstream outages paralyzing logistics or customer support).

RTO & RPO TIER CLASSIFICATION REFERENCE

STANDARD TARGETS

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

BUSINESS FUNCTION IMPACT RANKING & RECOVERY TIER REGISTER

WORKSHEET

Business Function / System Asset	Direct Financial Impact ($/hr, Sales Loss, SLA Penalty)	Regulatory & Fiduciary Rules (SEC 4d / DORA 4h / FFIEC 36h)	Cascading Failure Effects (Downstream Workflows)	Assigned Tier (0 / 1 / 2 / 3)	Target RTO & Target RPO
Customer Payment Gateway / Billing	High transactional loss; contractual SLA breach	SEC 4-day material impact; DORA 4h notice	Paralyzes all customer checkouts and renewals	Tier 0	RTO < 15m / RPO ~0
Core Production Relational Database	Halts platform operations; immediate churn	DORA 4h incident filing; FFIEC notification	Cascades to API, mobile apps, customer portal	Tier 0	RTO < 30m / RPO ~0
Customer Support & Ticketing Portal	SLA breach on enterprise customer contracts	Fiduciary reporting / customer SLA disclosures	Blocks incoming incident response / outreach	Tier 1	RTO < 4h / RPO < 15m
Inventory & Supply Logistics System	Delayed fulfillment; warehouse idle overtime	Downstream commercial contract penalties	Paralyzes physical distribution & shipping	Tier 1	RTO < 4h / RPO < 15m
Enterprise Cloud IaC & Core Middleware	Internal engineering blockage; deployment stall	Internal audit and operational compliance	Blocks staging, testing, and continuous delivery	Tier 2	RTO < 12h / RPO < 4h
Internal Business Intelligence & Reporting	Delayed executive dashboards; low immediate loss	Periodic compliance reporting (non-immediate)	No immediate external customer disruption	Tier 2	RTO < 24h / RPO < 4h
Internal Staff Intranet & Knowledge Base	Minimal direct financial loss; internal friction	No statutory notification mandates	Employees utilize temporary offline workarounds	Tier 3	RTO > 48h / RPO < 24h
Archived Financial Records & Tax Data	Zero daily operational impact; historical data	Statutory retention (IRS/audit) periodic access	None; static historical archive	Tier 3	RTO > 72h / RPO < 24h
[Custom System Asset 1]				Tier ___	RTO: ___ / RPO: ___
[Custom System Asset 2]				Tier ___	RTO: ___ / RPO: ___

BIA Lead Assessor: _____ Executive Sponsor Approval: _____ Assessment Date: _____

RECOVERY CHOICE SELECTOR (COLD, WARM, HOT & CLOUD / DRAAS)

ARCHITECTURE SELECTION

Evaluation Mandate: Select the recovery facility posture based on geographical risk separation, network latency, and operational cost. Record which posture each service uses and where data copies reside:

System / Business Function	Selected Posture (Cold / Warm / Hot / Cloud)	Primary Data Location vs. Secondary Copy Location	Replication / Provisioning Mechanism	Specific Justification / Cost Rationale
Payment Gateway / Auth	Hot Standby (Cloud Multi-Region)	Primary: AWS us-east-1 Secondary: AWS us-west-2	Synchronous active-active multi-region; GSLB automatic failover	Tier 0 revenue defense justifies continuous multi-region capacity
Core Production Database	Hot / Warm Standby	Primary: Cloud Region A Secondary: Cloud Region B	Continuous asynchronous replication; pre-scripted container spin-up	Tier 1 RTO < 2h; replication catch-up logs verified every 5 min
Customer Portal & API Services	Warm Standby / DRaaS	Primary: Production VPC Secondary: Disaster Recovery VPC	Automated IaC Terraform/Ansible; warm replica containers on standby	Tier 1 recovery; balances standby infrastructure cost against SLA
Analytics & Data Warehouse	Cold Standby (Cloud Snapshot)	Primary: Analytical Store Secondary: Remote Cloud Object Vault	Point-in-time snapshot restore from cloud object vault via automated scripts	Tier 2 RTO 12-24h; non-critical system does not justify hot standby
Internal Administrative Apps	Cold Standby / Bare-Metal	Primary: On-Prem / Local Host Secondary: Encrypted Offsite Archive	Periodic object archive restore; manual reprovisioning	Tier 3 RTO > 48h; low downtime cost allows bare-metal rebuild
[System Asset 1]	[ ] Cold [ ] Warm [ ] Hot [ ] Cloud	Pri: _____ Sec: _____	_____	_____
[System Asset 2]	[ ] Cold [ ] Warm [ ] Hot [ ] Cloud	Pri: _____ Sec: _____	_____	_____

MODERN BACKUP ARCHITECTURE COMPLIANCE AUDIT (THE 3-2-1-1-0 RULE)

RANSOMWARE & WIPER DEFENSE

Adversaries compromise online backup servers prior to deploying payload encryption. Document verifiable evidence for all 5 controls:

3-2-1-1-0 Rule Control	Technical Specification Required	Implementation Evidence & System Path / Account Details	Compliance Status
3 Copies of Data	At least 3 independent copies of critical production data (1 primary + 2 backup sets).	Copy 1 (Live Production): _____ Copy 2 (Local Snapshot): _____ Copy 3 (Remote Backup Set): _____	[ ] VERIFIED [ ] DEFICIENT
2 Different Media Types	At least 2 distinct storage technologies (e.g. enterprise SAN flash block + cloud object).	Media Type A (Primary Block/Flash): _____ Media Type B (Cloud Object Store): _____	[ ] VERIFIED [ ] DEFICIENT
1 Copy Stored Offsite	At least 1 backup copy in physically separated location / alternate cloud region.	Remote Facility / Alternate Cloud Region: _____ Geographic Hazard Zone Separation Distance: _____	[ ] VERIFIED [ ] DEFICIENT
1 Copy Immutable or Air-Gapped	Protected by WORM storage with Object Lock compliance, or isolated out-of-band air-gapped vault in separate account with separate credentials.	WORM Object Lock Compliance Policy: [ ] ENABLED Dedicated Out-of-Band Account / Vault ID: _____ Credential Isolation: Separate root credentials verified [ ] YES	[ ] VERIFIED [ ] DEFICIENT
0 Restoration Errors	Zero unrecoverable errors via automated daily checksum validations and recurring sandbox restores.	Automated Daily Checksum Verification Script: _____ Last End-to-End Sandbox Restore Date: _____ Unrecoverable Checksum Error Rate: [0.00%] Verified	[ ] VERIFIED [ ] DEFICIENT

Infrastructure Lead Sign-off: Backup Architect Sign-off: Audit Date:

PRINTABLE & FILLABLE WORKBOOK • $7 TIER
Current version — Nov 2, 2026. Update history: https://continuityhub.org/disaster-recovery-planning-complete-professional-guide/

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

RUNBOOK USABILITY

The 3:00 AM Standard: Disaster recovery runbooks must be executable by the engineer on call at 3:00 AM under conditions of high stress, imperfect information, and severe operational pressure. A plan that requires undocumented tribal folklore or institutional memory possessed solely by the primary architect fails the stranger test. Audit your runbooks against the four mandatory components:

1. DISASTER DECLARATION AUTHORITY

ESCALATION THRESHOLDS

- ☐ **Named Role Titles:** Explicitly names CIO, VP of Engineering, or DR Incident Commander empowered to authorize failover.
- ☐ **Objective Threshold Defined:** Specific operational trigger documented (e.g. uncontained database corruption > 30 min approaching RTO).
- ☐ **Escalation Path:** Contact path with secondary and tertiary delegates if primary commander is unreachable.

Primary Declaration Authority: _____
Objective Failover Cutover Threshold: _____

2. OUT-OF-BAND COMMS & SECURE ACCESS

INDEPENDENT ACCESS

- ☐ **Network Independence:** Emergency comms independent of disrupted corporate SSO, Slack, and internal email.
- ☐ **Pre-Authenticated Channels:** Dedicated secure Signal group or secondary cloud tenant configured and tested.
- ☐ **Hard-Copy Vault Credentials:** Emergency root and recovery credentials stored in tamper-evident physical hardware vaults.

4. THE FAILBACK PROTOCOL & SUPPLY CHAIN

REVERSE CUTOVER

- ☐ **Data Resynchronization Workflow:** Procedures to replicate modified transactions from secondary recovery site back to repaired primary facility.
- ☐ **Transaction Reconciliation Procedures:** Verified scripts to detect and resolve transactional conflicts incurred during disaster window.
- ☐ **Scheduled Maintenance Window:** Planned reverse cutover window to prevent secondary operational outage.
- ☐ **Supply Chain Disruption Coordination:** Emergency liaison protocols where physical facility closures affect supporting logistics or third-party vendors.

Failback Resync Script: _____
Supply Chain Incident Coordinator: _____

3. DETERMINISTIC STEP-BY-STEP TECHNICAL SEQUENCING AUDIT (COPY-PASTE COMMANDS)

CHRONOLOGICAL ORDER

Execution Step	Runbook Requirement & Technical Objective	Verification Status / Artifact Location	Stranger Test
Step 1: Traffic Quiescence	Divert incoming production traffic or place applications into maintenance mode to halt transactional writes before failover.	Command / Runbook Section: `$ traffic-control --mode maintenance --quiesce`	[ ] PASS [ ] FAIL
Step 2: Replication Verification	Validate replication catch-up logs, confirm replica data consistency, and break replication pairing to promote secondary database to primary.	Verification Query / Promotion Script: `$ db-replica --verify-sync && db-promote --primary`	[ ] PASS [ ] FAIL
Step 3: Infrastructure Provisioning	Spin up container clusters or compute virtual machines via automated infrastructure-as-code (Terraform/Ansible) manifests.	Automated IaC Repository / Manifest Path: `$ terraform apply -target=module.dr_cluster -auto-approve`	[ ] PASS [ ] FAIL
Step 4: Network & DNS Cutover	Update global server load balancers (GSLB) or modify external DNS A/CNAME records with pre-reduced Time-to-Live (TTL) values.	GSLB API Call / DNS Routing Automation: `$ gslb-cli --pool dr-secondary --switch-active --ttl 60`	[ ] PASS [ ] FAIL
Step 5: Automated Health Checks	Execute automated synthetic transaction tests before reopening traffic gates to external public users.	Synthetic Testing Suite / Health Validation: `$ run-synthetic-tests --env=dr --gate=open-on-pass`	[ ] PASS [ ] FAIL

Runbook Primary Author: _____ Independent Peer Reviewer (Stranger): _____ Audit Date: _____

THE TESTING LAW: "A RECOVERY THAT HAS NOT BEEN RUN IS A HYPOTHESIS"

EXERCISE LAW

Testing confirms recovery time (RTO) and recovery point (RPO) against the last copy, not against the architecture diagram. **Hard Rule:** *Do not file the test as a pass if users could not actually work.* Record every gap and update the plan. Progress through the 3-level exercise continuum:

1. Tabletop Walkthrough (Semi-Annual): Cross-functional leads talk through disaster scenarios step-by-step; validates roles, escalation, and procedural ambiguities.

2. Functional & Simulation (Annual): Sandbox execution without live traffic; restores immutable snapshots, measures real duration vs RTO; uncovers storage bottlenecks, missing env vars, expired SSL/TLS certs.

3. Full-Scale Chaos Drills (Annual - Tier 0): Controlled maintenance windows; terminates primary cloud regions, severs replication, chaos engineering (Chaos Mesh / AWS FIS).

ANNUAL EXERCISE CONTINUUM SCHEDULE

CADENCE PLANNING

Exercise Classification	Target Cadence	Target Scenario & Systems in Scope	Scheduled Window	Exercise Coordinator
Tabletop Walkthrough #1	Semi-Annual (H1)	Primary Data Center Ransomware & Backup Wiper Attack	Target: Q1 / April 15	Lead Continuity Architect
Tabletop Walkthrough #2	Semi-Annual (H2)	Cloud Region Complete Fiber Cut & Storage Vault Loss	Target: Q3 / October 10	Incident Response Commander
Functional Sandbox Simulation	Annual	Full Database Snapshot Restore & Container Orchestration	Target: Q2 / June 20	Lead Database Administrator
Full-Scale Interruption / Chaos	Annual (Tier 0)	Live Region Termination & Automated GSLB Cutover	Target: Q4 / November 14	VP Engineering / Infrastructure

DISASTER RECOVERY TEST EXECUTION LOG & AFTER-ACTION REPORT (AAR) REGISTER

TEST LOG

Test Date	Exercise Level & Scenario	Target RTO / RPO vs. Actual Duration Achieved	Gaps & Deficiencies Uncovered (Throughput, SSL, Env Vars, Replication)	User Work Capable?	AAR Ref & Remediation Milestone Owner
2026-04-12	Tabletop: Ransomware Wiper Scenario	Target RTO: 2h / RPO: 15m Theoretical: 2h 45m	Ambiguity in declaration authority delegation; missing out-of-band contact for secondary DBA	[ ] YES [x] NO (Tabletop)	AAR-2026-01 CAP Owner: IT Ops Lead
2026-06-18	Functional: Cloud Snapshot Sandbox Restore	Target RTO: 4h / RPO: 1h Actual: 3h 12m (Passed)	Discovered expired SSL wildcard cert on DR load balancer; storage throughput throttling on snapshot restore	[x] YES [ ] NO	AAR-2026-02 CAP Owner: SecOps Lead
2026-10-22	Chaos Drill: AWS Region Kill Simulation	Target RTO: 15m / RPO: 0m Actual: 18m 40s (Exceeded)	Container spin-up delayed due to missing environment variable in staging manifest; GSLB TTL cached 5m	[x] YES [ ] NO	AAR-2026-03 CAP Owner: DevOps Lead
[Test 1]		Target: _____ / _____ Actual: _____ / _____		[ ] YES [ ] NO	AAR-____ Owner: _____
[Test 2]		Target: _____ / _____ Actual: _____ / _____		[ ] YES [ ] NO	AAR-____ Owner: _____

Exercise Evaluation Director: _____ Lead Systems Architect: _____ Log Date: _____

KEEP THE PLAN CURRENT: THE 4 CONTINUOUS GOVERNANCE TRIGGERS

GOVERNANCE TRIGGERS

The Currency Imperative: 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. Static binders become obsolete within months. Enforce plan revisions using four continuous governance triggers:

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

2. Post-Incident & Exercise Remediation: Near-miss outages or tabletop exercise gaps mapped to Corrective Action Plans (CAPs) with strict 30-day update deadlines.

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

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

CONTINUOUS PLAN CURRENCY REVIEW & CHANGE LOG

CURRENCY REGISTER

Review Date	Governance Trigger Event	Systems / Runbooks Impacted	Specific Changes Applied & Technical Modifications	Author & Reviewing Architect	30-Day CAP Closeout
2026-02-14	Architecture Migration Trigger	Core Relational Database Runbook	Updated failover scripts for migration from on-prem PostgreSQL to AWS Aurora Multi-Region cluster.	DBA Lead / Lead Architect	[x] COMPLETE [ ] PENDING
2026-05-10	Post-Exercise CAP Remediation	DNS Cutover & Comms Runbook	Resolved AAR-2026-01 gap: added Signal out-of-band comms group and delegated failover role to VP Eng.	SecOps / Incident Cmdr	[x] COMPLETE (Day 28) [ ] PENDING
2026-07-15	Post-Incident Near-Miss Outage	Staging Snapshot Restore Script	Resolved AAR-2026-02 gap: updated automated wildcard SSL cert renewal in DR Terraform manifest.	DevOps Lead / Infra Head	[x] COMPLETE (Day 22) [ ] PENDING
2026-09-01	Annual Scheduled Recertification	Enterprise BIA & All 4 Runbook Tiers	Annual formal recertification: verified RTO/RPO targets against updated business SLA contracts.	All App Owners / CIO	[x] COMPLETE [ ] PENDING
2026-10-28	CI/CD Automated Verification	Terraform IaC Deployment Manifests	Automated pipeline alert: added missing backup tagging policy and immutable S3 Object Lock to new microservice.	Automated CI/CD / DevOps	[x] COMPLETE (Day 1) [ ] PENDING
[Review 1]	[ ] Migration [ ] CAP [ ] Annual [ ] CI/CD	_____	_____	_____	[ ] COMPLETE [ ] PENDING
[Review 2]	[ ] Migration [ ] CAP [ ] Annual [ ] CI/CD	_____	_____	_____	[ ] COMPLETE [ ] PENDING
[Review 3]	[ ] Migration [ ] CAP [ ] Annual [ ] CI/CD	_____	_____	_____	[ ] COMPLETE [ ] PENDING

Lead Continuity Officer: _____ Chief Information Officer / VP Eng: _____ Recertification Cycle: 2026 Annual