BRISKDATA ENGINEERING TEMPLATE | DOC ID: BD-GOV-DRP-005 | ADAPTABLE TEMPLATE

IT Disaster Recovery Plan (IT DRP) Template

Program Governance, Business Impact Tiering, Backup Isolation, Vendor Directory, and Drill Cadence

PROGRAM PLAN VS. SYSTEM RUNBOOK

This IT Disaster Recovery Plan establishes organization-wide authority, Business Impact Analysis (BIA) tiers, vendor escalation paths, and exercise schedules. Step-by-step technical failover commands belong in individual system runbooks (see BD-OPS-DR-001) linked from Section 2.

1. Plan Governance and Activation Authority

Governance Field	Organization Entry
Organization & Scope	[Organization Name - Corporate IT, Cloud Infrastructure, and Production Workloads]
DR Program Owner	[Name / Title, e.g., CTO / VP Infrastructure / IT Director]
Primary Declaration Authority	[Role(s) authorized to declare a formal disaster and approve live failover]
Alternate Authority	[Designated delegate if primary authority is unreachable]
Last Reviewed & Next Scheduled Test	Reviewed: [YYYY-MM-DD] | Next Exercise: [YYYY-MM-DD]

2. Business Impact Analysis (BIA) and Workload Tiering

Replace the bracketed impact, RTO, and RPO entries with targets approved by business and technical owners. Example tier descriptions below illustrate typical ordering.

Tier	Representative Workloads	Estimated Business Impact	Target RTO	Target RPO	Linked Runbook
Tier 0	Identity provider (SSO/MFA), core DNS, firewall/routing, password vault.	[Insert operational impact]	[e.g., < 1 hr]	[Near-zero / Config]	[BD-OPS-DR-000]
Tier 1	Primary customer application, billing/ERP database, clinical/order intake.	[Insert hourly financial/ops impact]	[e.g., 1 - 4 hrs]	[e.g., <= 15 min]	[BD-OPS-DR-001]
Tier 2	Corporate email, help desk, internal reporting, payroll, file collaboration.	[Insert daily operational impact]	[e.g., 4 - 12 hrs]	[e.g., <= 4 hrs]	[BD-OPS-DR-002]
Tier 3	Internal archives, non-production staging/dev, historical analytics.	[Low immediate impact]	[e.g., 24 - 72 hrs]	[e.g., 24 hrs]	[BD-OPS-DR-003]

3. Backup Isolation and Recovery Readiness Standards

- **Off-Site and Immutable Copies:** Maintain primary backups plus an off-site or cross-account copy protected by immutability controls (such as S3 Object Lock Compliance mode or hardened immutable repositories) so retention windows cannot be shortened during an account compromise.
- **Separated Administrative Identity:** Backup storage and recovery consoles must use dedicated authentication and hardware MFA separate from the primary corporate Active Directory or single cloud root account they protect.

- **Encryption Key Custody:** Store backup decryption keys and emergency recovery credentials in an out-of-band vault accessible when primary systems are offline.

4. Critical Vendor, Carrier, and External Counsel Directory

Vendor Category	Provider Name	Account / Contract ID	Emergency Contact Path	Agreed Support Tier
Cloud / Hosting Provider	[AWS / Azure / GCP / Host]	[Account ID]	[Support Portal / Phone]	[Insert agreed tier]
Identity & Productivity	[Microsoft 365 / Google]	[Tenant ID]	[Break-glass admin + Support]	[Insert agreed tier]
Primary & Secondary ISP	[Carrier Names]	[Circuit IDs]	[NOC Phone]	[Insert agreed SLA]
Cyber Insurance & Counsel	[Carrier / Law Firm]	[Policy Number]	[24/7 Hotline]	[Notify per policy]

5. Recovery Exercise Schedule and Evidence Log

Exercise Type	Agreed Cadence	Systems Covered	Evidence Recorded	Last Completed
Isolated Backup Restore	[Monthly / Quarterly]	[Tier 1 & Tier 2 databases/servers]	Timestamped restore log, integrity query output	[YYYY-MM-DD]
Tabletop Scenario Review	[Semi-Annual / Annual]	[Executive, IT, Legal, Communications]	Attendance record, decision log, open action items	[YYYY-MM-DD]
Parallel Functional Failover	[Annual or Major Change]	[Tier 0 / Tier 1 workloads]	Measured RTO & RPO vs target, signed review report	[YYYY-MM-DD]

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.