

Complete Disaster Recovery & Business Continuity Guide

Enterprise Resilience Planning | August 04, 2025



Recovery Objectives & Metrics

| System Tier | RTO (Recovery Time) | RPO (Data Loss) | Priority |
|--|---------------------|-----------------|-----------|
| Tier 1 - Critical Payment processing, authentication | 15 minutes | Zero | Immediate |
| Tier 2 - Essential Customer databases, email | 1 hour | 15 minutes | High |
| Tier 3 - Important Internal tools, reporting | 4 hours | 1 hour | Medium |
| Tier 4 - Standard Archives, development | 24 hours | 24 hours | Low |

Emergency Response Contacts

DR Team Lead: [Name] - [Phone] - Available 24/7

IT Operations: [Name] - [Phone] - Primary responder

Security Team: [Name] - [Phone] - Incident response

Communications: [Name] - [Phone] - Stakeholder updates

Vendor Support: [Company] - [Phone] - Priority ticket

Executive Sponsor: [Name] - [Phone] - Escalation

Phase 1: Preparation & Prevention

Implement automated backup strategy Ongoing

3-2-1 rule: 3 copies, 2 different media, 1 offsite. Incremental hourly, full daily

Configure high availability architecture Ongoing

Active-active clustering, load balancing, automatic failover, geo-redundancy

Document all system configurations Ongoing

Infrastructure as Code, runbooks, network diagrams, dependency mapping

Establish monitoring and alerting Ongoing

Real-time monitoring, predictive analytics, escalation chains, SLA tracking

Create disaster recovery workspace Ongoing

War room setup, remote access tools, communication channels, documentation repository

Maintain vendor support contracts Ongoing

Priority support agreements, spare hardware, cloud burst capacity, SLAs



Phase 2: Incident Detection & Assessment



Activate incident response team

0-5 min

Alert via automated system, SMS, phone tree. Confirm availability



Assess disaster scope and impact

5-15 min

Affected systems, data loss potential, business impact, recovery requirements



Declare disaster recovery status

15-30 min

Severity level (1-5), activate DR plan, notify stakeholders, initiate communications



Establish command center

30 min

Physical/virtual war room, communication bridges, status dashboards, logging



Document timeline and decisions

Continuous

Incident log, decision rationale, resource allocation, compliance records



Phase 3: System Recovery

Infrastructure Recovery



Activate backup infrastructure 0-1 hour

Cloud failover, standby data center, reserved capacity activation



Restore network connectivity 1-2 hours

VPN setup, firewall rules, DNS updates, routing tables



Deploy compute resources 2-4 hours

Virtual machines, containers, auto-scaling groups, load balancers

Data Recovery



Verify backup integrity Immediate

Checksum validation, corruption testing, recovery point verification



Restore databases 1-4 hours

Point-in-time recovery, transaction log replay, consistency checks



Synchronize file systems 2-6 hours

User data, application files, configuration, media assets



Validate data integrity 4-8 hours

Application testing, data reconciliation, audit trails

Application Recovery



Deploy application stack 2-4 hours

Web servers, application servers, microservices, APIs



Configure service dependencies 3-6 hours

Database connections, third-party integrations, message queues

⚡ Perform smoke testing 4-8 hours

Critical path testing, user acceptance, performance validation

Phase 4: Service Restoration

⚡ Restore services by priority tier Staged

Tier 1 first, progressive restoration, dependency management

⚡ Update DNS and routing 1-2 hours

TTL considerations, CDN purge, geographic routing

⚡ Enable user access gradually Phased

Internal users, beta group, percentage rollout, full access

⚡ Monitor system performance Continuous


Resource utilization, response times, error rates, user experience


⚡ Communicate restoration status Hourly


Status page updates, customer notifications, internal briefings

Phase 5: Communication Plan


Internal Communications


 Executive briefing Every 30 min
Impact assessment, recovery progress, business decisions, resource needs


 Employee notifications Hourly
Work instructions, remote access, safety information, return to work


 Technical team coordination Continuous
Slack/Teams channel, conference bridge, task assignments

External Communications

 Customer notifications Within 1 hour
Email, SMS, status page, social media, support tickets

 Vendor coordination As needed
Support tickets, escalations, resource requests, SLA claims

 Regulatory reporting Per requirements
Breach notifications, compliance reports, audit documentation

 Media relations As needed
Press releases, spokesperson briefing, social media management

✓ Phase 6: Recovery Validation

⚡ Conduct system health checks **Post-recovery**
All services operational, performance metrics normal, no data corruption

⚡ Verify backup systems **Within 24 hours**
Ensure backups resume, test restore capability, update documentation

⚡ User acceptance testing **Within 48 hours**
Key stakeholder sign-off, functionality verification, performance acceptance

⚡ Security assessment **Within 72 hours**
Vulnerability scan, access review, incident analysis, forensics if needed

📅 Phase 7: Post-Incident Activities

⚡ Conduct post-mortem analysis **Within 1 week**
Root cause analysis, timeline review, decision evaluation, improvement areas

⚡ Update DR documentation **Within 2 weeks**
Lessons learned, procedure updates, contact changes, new dependencies

⚡ Calculate financial impact **Within 2 weeks**
Downtime costs, recovery expenses, insurance claims, SLA credits

⚡ Implement improvements **30-90 days**
Technology upgrades, process changes, training updates, tool enhancements

⚡ Schedule next DR test **Quarterly**
Tabletop exercise, partial failover, full DR test, surprise drills

Critical Success Factors

- ✓ Regular testing - Quarterly DR drills minimum
- ✓ Documentation currency - Monthly review and updates
- ✓ Team training - All staff know their roles
- ✓ Vendor relationships - Pre-negotiated support agreements
- ✓ Executive support - Budget and resources allocated
- ✓ Continuous improvement - Learn from every incident

Essential DR Tools & Resources

Backup & Replication Software

Veeam, Commvault, AWS Backup, Azure Site Recovery

Monitoring & Alerting Platforms

PagerDuty, Datadog, New Relic, Prometheus/Grafana

Communication Tools

Slack, Microsoft Teams, Zoom, mass notification systems

Documentation Repositories

Confluence, SharePoint, Git, offline copies on USB

Cloud Disaster Recovery

AWS Disaster Recovery, Azure Site Recovery, GCP DR

Testing & Validation Tools

Chaos engineering, load testing, synthetic monitoring

© 2025 GooyIT. All rights reserved.

Version 4.0 | ISO 22301 Aligned | Last Updated: August 2025