Disaster Recovery Testing Checklist

The Quarterly DR Drill Framework from Ascendro's Operations Team

Pre-Drill Planning (Week 1)

Scenario Selection

- □ Define disaster scenario (server failure, data corruption, ransomware, regional outage)
- □ Identify systems to be tested
- □ Determine testing window and impact assessment
- □ Assign drill roles and responsibilities
- □ Review and update contact lists

Documentation Review

- □ Verify DR runbooks are current
- □ Confirm backup locations and access credentials
- □ Review Recovery Time Objectives (RTO) targets
- □ Review Recovery Point Objectives (RPO) targets
- □ Update system architecture diagrams

Communication Planning

- □ Draft stakeholder notification templates
- □ Prepare status update schedule
- □ Define escalation matrix
- □ Set up war room (physical/virtual)
- □ Create incident tracking spreadsheet

Execution Phase (Week 2)

Initial Response (First 15 Minutes)

- □ Trigger drill without full team warning (if surprise drill)
- □ Start incident timer
- □ Activate incident response team
- □ Establish communication channels
- □ Begin incident documentation

Assessment Phase (15-30 Minutes)

- □ Identify affected systems

- □ Determine data loss potential
- □ Assess business impact
- □ Review available backups
- □ Validate recovery resources availability

Recovery Execution (30 Minutes - 2 Hours)

- □ Initiate failover procedures
- □ Begin backup restoration
- □ Execute service recovery in priority order:
- □ Critical: Authentication, Database
- □ High: Application services, APIs
- □ Medium: Monitoring, logging
- □ Low: Non-critical services
- □ Monitor recovery progress
- □ Document any deviations from runbooks

Validation Phase

- □ Verify data integrity
- □ Test application functionality
- □ Confirm all services restored
- □ Check monitoring and alerting systems
- □ Validate customer access

Measurement & Analysis (Week 3)

Key Metrics Collection

- □ Total recovery time (compare to RTO)
- □ Data loss window (compare to RPO)
- □ Time to first response
- □ Time to full recovery
- □ Number of escalations required
- □ Runbook accuracy (% followed vs. improvised)

Recovery Quality Assessment

- □ Services restored correctly: ___%
- □ Data integrity maintained: Yes/No
- □ Customer impact minimized: Yes/No
- □ Communication effectiveness: 1-10

- □ Team coordination: 1-10

Issue Documentation

- □ List all problems encountered
- □ Document workarounds used
- □ Identify missing procedures
- □ Note tool/access issues
- □ Record communication breakdowns

Post-Drill Improvements (Week 4)

Root Cause Analysis

- □ Conduct post-mortem meeting
- □ Identify top 3 improvement areas
- □ Assign action items with owners
- □ Set completion deadlines
- □ Update risk register

Documentation Updates

- □ Revise DR runbooks based on findings
- □ Update contact lists
- □ Improve recovery procedures
- □ Document new dependencies discovered
- □ Create/update automation scripts

Process Improvements

- □ Optimize backup strategies
- □ Adjust monitoring thresholds
- □ Enhance alerting rules
- □ Improve team training materials
- □ Schedule follow-up training if needed

Specific Scenario Tests

Scenario 1: Single Server Failure

- □ Simulate primary server crash
- □ Test automated failover
- □ Verify load balancer redirection

- □ Confirm session persistence
- □ Validate no data loss

Scenario 2: Database Corruption

- □ Corrupt test database
- □ Execute point-in-time recovery
- □ Verify transaction log replay
- □ Test data consistency checks
- □ Validate application reconnection

Scenario 3: Complete Regional Outage

- □ Simulate data center failure
- □ Execute cross-region failover
- □ Test DNS switching
- □ Verify data replication lag
- □ Confirm geo-redundancy

Scenario 4: Ransomware Attack

- □ Simulate encryption event
- □ Isolate affected systems
- □ Execute clean recovery
- □ Restore from immutable backups
- □ Verify security patches applied

Success Criteria Checklist

Must Pass (Critical)

- □ RTO achieved (<2 hours)
- □ RPO achieved (<1 hour)
- □ No permanent data loss
- □ All critical services restored
- □ Customer authentication working

Should Pass (Important)

- □ Communication plan executed
- □ Runbooks 80% accurate
- □ Monitoring restored
- □ Incident documented properly

- [ ] Team responded within SLA

Nice to Have (Optimal)

- [ ] Zero customer complaints
- [ ] Automated recovery worked
- [ ] No manual interventions
- [ ] Under-budget resource usage
- [ ] Lessons learned documented same day

Quarterly Schedule Template

Q1 Drill: Basic Failure

- Focus: Single component failure
- Goal: Team familiarization
- Duration: 2 hours

Q2 Drill: Complex Scenario

- Focus: Multiple system failure
- Goal: Coordination testing
- Duration: 4 hours

Q3 Drill: Surprise Drill

- Focus: Unannounced test
- Goal: Real readiness assessment
- Duration: As needed

Q4 Drill: Full DR Test

- Focus: Complete site failover
- Goal: Annual certification
- Duration: Full day

Red Flags to Watch For

During Execution:

- ⚠️ Backup access takes >30 minutes
- ⚠️ Team can't find runbooks

- ⚠️ Critical passwords unknown
- ⚠️ Recovery tools not installed
- ⚠️ Network configurations missing

Post-Drill:

- 🚨 RTO missed by >50%
- 🚨 Data corruption discovered
- 🚨 Services won't start
- 🚨 Monitoring blind spots found
- 🚨 Communication breakdown

Tools & Resources Needed

Essential Tools

□ Backup software access
□ Cloud console credentials
□ Database management tools
□ Network diagnostic tools
□ Communication platform (Slack/Teams)

Documentation Required

□ DR runbooks (current version)
□ Network diagrams
□ Application dependencies map
□ Contact list (24/7)
□ Vendor support contracts

Team Resources

□ Incident Commander
□ Technical Lead
□ Communications Lead
□ Business Liaison
□ Documentation Scribe

Ascendro's Pro Tips

1. Make It Real: Don't just talk through scenarios - actually break things (in a controlled way).

2. Time Everything: If you're not measuring, you're not improving.

3. Rotate Roles: Different team members should lead each quarterly drill.

4. External Dependencies: Test vendor support response times during drills.

5. Document Everything: The worst time to write a runbook is during a real disaster.

6. Celebrate Success: When drills go well, recognize the team. When they don't, celebrate the learning.

This checklist is based on Ascendro's experience managing 10+ production SaaS applications with 99.9% uptime SLA commitments and ITIL-based operational processes.

Need help implementing a DR testing program? Contact Ascendro's operations team for guidance on building resilient infrastructure and operational processes.