Resume - Jaecheol Lee

Jaecheol Lee

2025-12-24

Contents

1 Nextrade Securities Exchange - Disaster Recovery Plan

1.1 Executive Summary

Comprehensive disaster recovery plan ensuring business continuity for critical trading infrastructure. Achieved **2.5-hour DR test** (37% better than 4-hour target) with **zero data loss** through automated failover procedures.

Scope: Trading platform, clearing system, market data, surveillance **RTO Target**: 4 hours (achieved 2.5 hours) **RPO Target**: 15 minutes (zero data loss) **Test Frequency**: Quarterly (4 tests/year) **Compliance**: FSC requirements, ISO 22301 aligned

---

1.2 RTO/RPO Objectives

System	Classification	RTO Target	RPO Target	2025 Achievement
Trading Platform	Critical	4 hours	15 min	**2.5 hours**
Clearing System	Critical	6 hours	30 min	4.2 hours
Market Data Feed	Critical	2 hours	5 min	1.8 hours
Surveillance	Important	8 hours	1 hour	6 hours
Back Office	Important	12 hours	4 hours	10 hours
Website/Portal	General	24 hours	8 hours	18 hours

Overall Performance: All systems recovered within target RTO/RPO

1.3 Disaster Scenarios

1.3.1 Scenario 1: Primary Data Center Failure

Cause: Power outage, fire, flood, physical breach **Impact**: Complete loss of primary site **Recovery**: Failover to DR site (2.5 hours)

1.3.2 Scenario 2: Ransomware Attack

Cause: Malware encryption of production systems **Impact**: Systems unavailable, data encrypted **Recovery**: Restore from immutable backups (4 hours)

1.3.3 Scenario 3: Network Connectivity Loss

Cause: ISP outage, DDoS, fiber cut **Impact**: External access unavailable **Recovery**: Failover to secondary ISP + BGP rerouting (15 minutes)

1.3.4 Scenario 4: Database Corruption

Cause: Software bug, hardware failure, human error **Impact**: Transaction data inconsistency **Recovery**: Point-in-time restore from backups (2 hours)

1.3.5 Scenario 5: Cyber Attack with Data Breach

Cause: APT, insider threat, credential theft **Impact**: System compromise, potential data exfiltration **Recovery**: Isolate + forensics + clean rebuild (8-12 hours)

1.4 DR Infrastructure

1.4.1 Primary Site (Production)

Location: Seoul Data Center (Gasan Digital Complex) - **Servers**: 150+ (physical + virtual) - **Storage**: Dell EMC Unity 600F (100TB all-flash) - **Network**: Dual 10Gbps links (active-active) - **Power**: N+1 redundancy, UPS + generator

1.4.2 DR Site (Standby)

Location: Busan Data Center (150km from primary) - **Servers**: 100+ (mirrored configuration) - **Storage**: Dell EMC Unity 400F (50TB all-flash) - **Network**: Dual 10Gbps links (active-active) - **Power**: N+1 redundancy, UPS + generator - **Replication**: Synchronous for critical systems

1.4.3 Backup Strategy

Primary Backups: Veeam Backup & Replication - **Full**: Weekly (Sunday 2 AM) - **Incremental**: Daily (2 AM) - **Retention**: 30 days local + 90 days offsite + 7 years archive (tape)

Offsite Storage: Immutable object storage (AWS S3 Glacier) - **Replication**: Daily (encrypted AES-256) - **Air-Gap**: Separate account, MFA required - **Test Restore**: Monthly validation

---

1.5 Recovery Procedures

1.5.1 Failover to DR Site (Scenario 1)

Phase 1: Declaration (10 minutes) 1. Incident Commander declares disaster 2. Notify recovery team (SMS + voice call) 3. Activate war room (Zoom + Slack) 4. Notify FSC within 1 hour

Phase 2: Assessment (20 minutes) 1. Verify primary site status (unreachable/damaged) 2. Check DR site readiness (power, network, storage) 3. Verify latest backup/replication timestamp 4. Confirm data consistency

Phase 3: Network Failover (30 minutes) 1. Update DNS records (TTL 60 seconds) 2. BGP route announcement (DR site IPs) 3. VPN gateway failover 4. Load balancer reconfiguration 5. Verify external connectivity

Phase 4: System Recovery (90 minutes) 1. Power on DR servers (priority order: DB → App → Web) 2. Start critical services (matching engine, order router, market data) 3. Verify database integrity (checksum validation) 4. Enable trading API endpoints 5. Run smoke tests (place test orders)

Phase 5: Verification (20 minutes) 1. Functional testing (end-to-end order flow) 2. Performance testing (latency < 50ms) 3. Data integrity checks (order book reconciliation) 4. User acceptance testing (5 pilot users) 5. Go/no-go decision

Phase 6: Go-Live (10 minutes) 1. Enable production traffic 2. Notify users (email + website banner) 3. Monitor closely (first 2 hours) 4. Incident log updates

Total Time: 2.5 hours (target 4 hours)

1.5.2 Ransomware Recovery (Scenario 2)

Phase 1: Isolation (15 minutes) 1. Disconnect infected systems from network 2. Disable network shares and backups 3. Block C2 domains on firewall 4. Capture forensic evidence

Phase 2: Assessment (30 minutes) 1. Identify encrypted systems/files 2. Determine ransomware variant (analysis) 3. Check backup availability (not encrypted) 4. Estimate recovery time

Phase 3: Eradication (60 minutes) 1. Wipe infected systems (secure erase) 2. Update all systems (OS patches, AV signatures) 3. Change all credentials (passwords, keys, tokens) 4. Block known IOCs (IPs, domains, hashes)

Phase 4: Restoration (120 minutes) 1. Restore systems from clean backups 2. Verify backup integrity (hash validation) 3. Apply security patches before production 4. Enable monitoring/alerting

Phase 5: Testing (30 minutes) 1. Malware scan on restored systems 2. Functional testing 3. Monitor for re-infection (48 hours)

Total Time: 4 hours

1.5.3 Network Failover (Scenario 3)

Automated Failover (<15 minutes) 1. Monitor detects primary ISP down (2 consecutive failed pings) 2. BGP automatically withdraws primary routes 3. Traffic fails over to secondary ISP 4. Monitoring alert sent (no human intervention required)

Manual Steps (if automation fails) 1. Verify both ISPs down (rare: dual failure) 2. Activate backup 4G/5G links (100Mbps capacity) 3. Notify ISPs for troubleshooting 4. Enable traffic prioritization (critical services only)

1.6 DR Test Results

1.6.1 2025 Q2 Test (2025-04-15)

Scenario: Primary data center failure **Duration**: 2 hours 32 minutes (target: 4 hours) **Success Criteria**: All critical systems restored **Results**: - Trading platform: 2h 18m (RTO 4h) - Clearing system: 2h 25m (RTO 6h) - Market data: 1h 45m (RTO 2h) - All data verified (zero loss) - Minor issue: VPN certificate mismatch (resolved in 12 minutes)

Improvements Applied: - Pre-load VPN certificates on DR site - Add automated DNS update script - Parallel server startup (reduced by 30 minutes)

1.6.2 2025 Q3 Test (2025-07-20)

Scenario: Ransomware attack simulation **Duration**: 3 hours 58 minutes (target: 4 hours) **Results**: - All encrypted systems identified - Clean backup restored successfully - No re-infection detected (48-hour monitoring) - IOC blocking automated

Improvements Applied: - Immutable backup validation (monthly) - Faster malware scan (SSD-optimized)

1.7 Monitoring & Alerting

1.7.1 DR Site Health Checks

Automated Checks (every 5 minutes): - DR site power status - Network connectivity (ping + bandwidth test) - Storage replication lag (<15 minutes) - Backup job success (daily) - Server heartbeats

Alerts (Slack + PagerDuty): - Replication lag >10 minutes → P1 alert - Backup job failure → P1 alert - DR site connectivity loss → P0 alert (immediate escalation)

1.7.2 Recovery Metrics

KPIs: - RTO Achievement: 100% (all systems within target) - RPO Achievement: 100% (zero data loss) - DR Test Pass Rate: 100% (4/4 tests passed) - Backup Success Rate: 99.8% (2 failures in 365 days) - Replication Lag: Avg 3.2 minutes (target <15 minutes)

1.8 Roles & Responsibilities

1.8.1 DR Team

Incident Commander: Security Lead (Jaecheol Lee) - Overall coordination and decision-making - FSC notification and communication - Go/no-go decision for go-live

Technical Lead: Infrastructure Manager - Execution of recovery procedures - System restoration and verification - Post-recovery monitoring

Database Lead: DBA - Database recovery and integrity checks - Transaction log analysis - Performance tuning post-recovery

Network Lead: Network Engineer - Network failover and routing - VPN/firewall reconfiguration - Connectivity verification

Communication Lead: Compliance Manager - User notification and status updates - FSC/regulator communication - Documentation and reporting

1.8.2 Escalation

```
Technical Issue → Technical Lead → Incident Commander → CTO → CEO (if >4h downtime)
```

1.9 Business Continuity

1.9.1 Critical Business Functions

Priority 1 (RTO <4 hours): - Order matching and execution - Market data distribution - Trade clearing and settlement

Priority 2 (RTO <8 hours): - Market surveillance - User account management - Customer support systems

Priority 3 (RTO <24 hours): - Reporting and analytics - Marketing website - Internal collaboration tools

1.9.2 Workarounds During Recovery

Manual Trading (if system unavailable): - Phone orders accepted (backup call center) - Manual order matching (emergency procedure) - Post-recovery electronic reconciliation

Communication Plan: - Website status page updates (every 30 minutes) - Email notifications to registered traders - Social media updates - FSC hourly updates (for >2 hour outages)

1.10 Compliance & Reporting

1.10.1 FSC Reporting Requirements

Incident Notification: - **Initial**: Within 1 hour of disaster declaration - **Progress**: Hourly updates until resolution - **Final**: Within 72 hours post-recovery

Report Contents: - Incident description and root cause - Systems affected and recovery status - Customer impact assessment - Corrective actions and timeline

1.10.2 Audit & Documentation

DR Test Reports (quarterly): - Test objectives and scenarios - Results and metrics (RTO/RPO achieved) - Issues identified and corrective actions - Evidence attachments (logs, screenshots)

Backup Logs (retained 7 years): - Backup job status (success/failure) - Restore test results (monthly validation) - Storage capacity and utilization

---

1.11 Continuous Improvement

1.11.1 Post-DR Test Actions

1. **Debrief Meeting** (within 48 hours)
   - What went well
   - What went wrong
   - Root cause analysis
2. **Action Items** (within 1 week)
   - Update DR procedures
   - Fix identified issues

- Schedule automation improvements

3. **Procedure Updates** (within 2 weeks)
   - Incorporate lessons learned
   - Update runbooks
   - Retrain team on changes
4. **Next Test Planning** (within 1 month)
   - Define next scenario
   - Schedule test date
   - Coordinate with business

1.12 Key Achievements

- **RTO Performance**: 37% better than target (2.5h vs 4h)
- **Zero Data Loss**: 100% RPO achievement across all tests
- **Test Success Rate**: 100% (4/4 tests passed in 2025)
- **Automation**: 70% of recovery steps automated
- **Compliance**: 100% FSC requirement satisfaction

Document: Compact DR Plan for Resume/Portfolio **Classification**: Internal Use **Version**: 1.0 Compact
Date: 2025-10-16 **Next Test**: 2025-10-30 **Contact**: 이재철 (Jaecheol Lee) | qws941@kakao.com