GRC205 Week 21 - Practical Lab Assignment

Data Center Disaster Recovery Simulation

Course: GRC205 - Incident Management and Business Continuity
Week: 21 (Dec 8 - Dec 14)
Topic: Business Continuity and Disaster Recovery
Assignment Type: Practical Simulation-Based Assignment
Due Date: End of Week 21
Estimated Time: 12-15 hours

Assignment Overview

In this immersive practical simulation, you will experience a realistic data center disaster scenario and lead the disaster recovery response for **FinanceFirst Bank**, a regional financial institution. You will make time-critical decisions, coordinate recovery activities, manage stakeholder communications, and document your actions throughout a multi-day disaster recovery operation.

This assignment tests your ability to apply BC/DR knowledge under realistic pressure, make sound decisions with incomplete information, coordinate cross-functional teams, and execute recovery procedures while balancing competing priorities. You will demonstrate practical mastery of disaster recovery execution, not just theoretical knowledge.

Simulation Format: This is a scenario-based simulation where you will receive information progressively throughout the scenario timeline. You must respond to each scenario phase with decisions and actions, then document your complete response in a comprehensive after-action report.

Organization Profile: FinanceFirst Bank

Company Overview: FinanceFirst Bank is a regional bank with $8.5 billion in assets, serving 250,000 customers across five states (Illinois, Indiana, Wisconsin, Iowa, Michigan). The bank operates 85 branch locations, employs 1,200 staff, and offers retail banking, commercial lending, wealth management, and mortgage services.

Technology Infrastructure:

Primary Data Center (Chicago, IL):

- 10,000 sq ft facility in downtown Chicago
- Hosts all production banking systems
- Redundant power (utility + generator + UPS)
- Redundant HVAC systems
- Dual internet connections from different providers

- Physical security with 24/7 monitoring

Disaster Recovery Site (Milwaukee, WI):

- Warm site with 120 miles separation from primary
- Infrastructure in place but requires data restoration and configuration
- Tested quarterly with tabletop exercises
- Last full DR test: 18 months ago (successful but took 14 hours to restore core banking)

Critical Systems:

System	Description	RTO	RPO	Current Backup
Core Banking System	Account management, transactions, balances	4 hours	15 minutes	Real-time replication to DR site
Online Banking Portal	Customer web access	2 hours	30 minutes	Hourly incremental backups
Mobile Banking App	Customer mobile access	2 hours	30 minutes	Hourly incremental backups
ATM Network	200 ATMs across 5 states	6 hours	1 hour	Hourly transaction log backups
Wire Transfer System	Domestic and international wires	4 hours	0 (no data loss acceptable)	Real-time replication
Loan Origination System	Mortgage and commercial loans	24 hours	4 hours	Nightly full backup
Email System	Corporate email (Microsoft 365)	8 hours	1 hour	Cloud-based (Microsoft manages)
Branch Teller System	In-branch transactions	4 hours	15 minutes	Real-time replication to DR site

Compliance and Regulatory Context:

- Federal Reserve oversight and examination
- FDIC insurance and reporting requirements
- GLBA (Gramm-Leach-Bliley Act) privacy requirements
- Bank Secrecy Act (BSA) and anti-money laundering (AML) compliance
- State banking regulations in five states
- Must notify regulators of significant operational disruptions within 4 hours

Business Context:

- Peak transaction periods: Weekday mornings (8-10 AM), lunch (12-1 PM), Friday afternoons
- Month-end processing: Critical for financial reporting and regulatory filings
- Wire transfer cutoff: 5:00 PM CT for same-day processing
- Quarterly earnings announcement: Next week (high visibility period)

Disaster Scenario: Primary Data Center Failure

Phase 1: Initial Event (Tuesday, 6:45 AM CT)

INCIDENT ALERT - PRIORITY 1

You are the Disaster Recovery Manager for FinanceFirst Bank. You receive an emergency call from the Night Operations Manager:

> *"We have a major problem at the Chicago data center. At 6:30 AM, a water main break on the street outside the building caused catastrophic flooding in the basement. Water has reached the first floor, where our data center is located. The facility manager reports 4-6 inches of standing water in the data center. Power has been cut to the entire facility as a safety precaution. All systems are down. The city says the water main break will take at least 12-18 hours to repair, and we don't know the full extent of damage yet."*

Current Status (6:45 AM):

- All production systems offline
- Primary data center inaccessible due to flooding and power outage
- DR site in Milwaukee is operational and ready
- Last successful backup replication: 6:15 AM (30 minutes ago)
- No injuries reported
- 15 IT staff on-site or en route to Chicago data center
- 10 IT staff available at DR site in Milwaukee
- Executive team not yet notified (they typically arrive at 8:00 AM)

Environmental Conditions:

- Heavy rain continuing (forecast: rain all day)
- Temperature: 38°F
- Chicago traffic: Heavy due to weather and morning rush hour

Immediate Considerations:

- Bank branches open at 9:00 AM (2 hours 15 minutes)
- Online and mobile banking currently unavailable
- ATM network offline
- Wire transfer deadline: 5:00 PM today
- 250,000 customers potentially affected

Your Response - Phase 1 (Due: Within 2 hours of incident)

Task 1.1: Initial Assessment and Decision (15 points)

Provide your immediate response to this scenario:

1. **Situation Assessment:** Analyze the current situation. What is the severity of this incident? What are the immediate business impacts? What information do you need that you don't currently have?
2. **DR Plan Activation Decision:** Should you activate the full disaster recovery plan? Provide your decision (YES/NO) with detailed justification. Consider the implications of activating DR (cost, effort, risk) versus attempting to restore the primary site.
3. **Initial Actions (First 30 Minutes):** List the specific actions you will take in priority order during the first 30 minutes. Who will you notify? What teams will you mobilize? What immediate steps will you direct?
4. **Communication Plan:** Draft the initial notification message you will send to:
    - ✓ Executive Leadership (CEO, CFO, CIO, COO)
    - ✓ Federal Reserve and FDIC (regulatory notification)
    - ✓ IT Recovery Teams
    - ✓ Branch Managers

Each message should be tailored to the audience, provide the necessary information, and clearly set expectations.

Phase 2: Recovery Execution (Tuesday, 9:00 AM - 12:00 PM)

SITUATION UPDATE - 9:00 AM

You have activated the disaster recovery plan. The DR team has mobilized at the Milwaukee site. You receive the following updates:

Good News:

- DR site infrastructure is operational
- Network connectivity to DR site is stable
- Backup data is intact and accessible
- Core banking system recovery has begun
- Executive team has been briefed and is supportive

Challenges:

- Core banking system recovery is taking longer than expected (estimated 6 hours instead of 4 hours)
- Online banking portal requires manual configuration that wasn't fully documented
- 3 key technical staff are stuck in traffic due to weather and won't arrive for 2 more hours
- Branch managers are calling asking when systems will be available
- Social media posts from customers complaining about online banking being down
- Local news has picked up the story: "FinanceFirst Bank Systems Down Due to Flooding"

Additional Information:

- Chicago data center assessment: Extensive water damage to equipment, estimated 5-7 days before facility is operational again
- Insurance adjuster en route to assess damage
- City confirms water main repair will take until 8:00 PM tonight

Stakeholder Pressure:

- CEO wants hourly updates and is concerned about reputational damage
- Chief Risk Officer is worried about regulatory implications
- Chief Customer Officer reports call center is overwhelmed (300% normal call volume)
- Branch managers report that customers are frustrated and some are threatening to switch banks

Your Response - Phase 2 (Due: Within 4 hours of Phase 1)

Task 2.1: Recovery Prioritization and Execution (20 points)

Document your recovery strategy and execution plan:

5. **System Recovery Prioritization:** Given the challenges, define the specific order in which you will recover systems. Justify your prioritization based on business impact, technical dependencies, and available resources.
6. **Resource Allocation:** You have 25 IT staff available (15 in Chicago, 10 in Milwaukee). How will you allocate these resources across recovery tasks? Create a resource assignment matrix showing who is working on what.
7. **Problem-Solving:** Address the specific challenges:
   - ✓ Core banking taking longer than expected: What actions will you take?
   - ✓ Online banking configuration issues: How will you resolve this?
   - ✓ Key staff delayed: How will you work around their absence?
8. **Timeline and Milestones:** Create a recovery timeline showing when you expect each critical system to be restored. Include key milestones and decision points.

Task 2.2: Stakeholder Management (15 points)

Manage the various stakeholder concerns:

9. **Executive Communication:** Draft an email update to the CEO and executive team (9:30 AM) providing status, challenges, revised timeline, and risk mitigation actions.
10. **Regulatory Communication:** Prepare a formal notification to regulators (Federal Reserve and FDIC) documenting the incident, impact, recovery actions, and expected restoration timeline.
11. **Customer Communication:** Draft a customer-facing statement for:
    - ✓ Website banner notification
    - ✓ Social media post
    - ✓ Branch signage
    - ✓ Call center talking points

12 **Media Management:** The local news wants a statement. Draft a brief media statement (3-4 sentences) that is honest but protects the bank's reputation.

13 **Internal Communication:** Create a message for all bank employees explaining the situation and what they should tell customers.

Phase 3: Complications and Decisions (Tuesday, 2:00 PM)

SITUATION UPDATE - 2:00 PM

Recovery is progressing, but new complications have emerged:

Recovery Status:

- Core banking system: 80% complete, expected online by 4:00 PM
- Online banking portal: Restored at 1:30 PM (limited functionality)
- Mobile banking: Restored at 1:45 PM
- ATM network: 60% operational (120 of 200 ATMs online)
- Wire transfer system: Not yet started (team focused on core banking)
- Branch teller system: Restored at 12:30 PM (branches now operational)

New Complications:

Complication 1: Data Integrity Issue The database team reports that the last backup before the incident (6:15 AM) has a corruption issue affecting approximately 2,000 customer accounts. The previous clean backup is from 11:45 PM last night (6.5 hours ago).

Options:

- **Option A:** Use the 11:45 PM backup (clean data but 6.5 hours of lost transactions)
- **Option B:** Use the 6:15 AM backup and manually correct the 2,000 affected accounts (estimated 8-12 hours of work)
- **Option C:** Delay core banking restoration while investigating the corruption (unknown time)

Complication 2: Wire Transfer Deadline It's now 2:00 PM and the wire transfer system isn't restored yet. Wire transfer cutoff is 5:00 PM (3 hours away). You have 47 pending wire transfers totaling $23.5 million that must be processed today to meet customer commitments and contractual obligations. Missing the deadline will result in:

- Significant customer dissatisfaction
- Potential breach of contract penalties
- Regulatory scrutiny
- Reputational damage

The wire transfer system requires 2 hours to restore and 30 minutes to process all pending wires.

Complication 3: Vendor Issue Your core banking software vendor (FiServ) is requiring a special license key to run the system at the DR site beyond 24 hours. The vendor's licensing team is not responding to urgent requests. Without the license key, the system will shut down at 6:30 AM tomorrow morning.

Complication 4: Staff Fatigue Your recovery team has been working for 8 hours straight. Several team members are showing signs of fatigue and making minor errors. You have backup staff available but they are less experienced with DR procedures.

Your Response - Phase 3 (Due: Within 6 hours of Phase 1)

Task 3.1: Critical Decision-Making (25 points)

Make and justify decisions for each complication:

14. **Data Integrity Decision:** Choose Option A, B, or C for the data corruption issue. Provide detailed justification for your decision considering:
    - ✓ Business impact of each option
    - ✓ Risk assessment
    - ✓ Customer impact
    - ✓ Regulatory implications
    - ✓ Resource requirements
15. **Wire Transfer Priority Decision:** How will you handle the wire transfer deadline? Options include:
    - ✓ Divert resources from core banking to prioritize wire transfers
    - ✓ Accept missing the deadline and focus on core banking
    - ✓ Attempt parallel recovery of both systems
    - ✓ Seek alternative wire transfer processing method
16. Justify your decision with risk-benefit analysis.
17. **Vendor Licensing Issue:** Develop a plan to resolve the vendor licensing issue. What specific actions will you take? Who will you escalate to? What is your backup plan if the vendor doesn't respond?
18. **Staff Management:** How will you address team fatigue while maintaining recovery momentum? Create a staffing plan for the next 12 hours including shift rotations, breaks, and backup resource deployment.

Task 3.2: Risk Management and Contingency Planning (10 points)

19. **Risk Register:** Create a risk register identifying the top 5 risks to successful recovery at this point in the scenario. For each risk, document:
    - ✓ Risk description
    - ✓ Probability (High/Medium/Low)
    - ✓ Impact (High/Medium/Low)

- ✓ Mitigation actions
- ✓ Contingency plan if risk materializes

20 **Go/No-Go Decision:** At what point would you decide to abandon the DR site recovery and pursue an alternative approach? Define your decision criteria and alternative options.

Phase 4: Final Recovery and Transition (Wednesday, 8:00 AM)

SITUATION UPDATE - Wednesday 8:00 AM (26 hours after incident)

Recovery Status:

- Core banking system: Fully operational at DR site since 5:30 PM Tuesday
- All customer-facing systems restored and operational
- Wire transfers: All 47 pending wires processed by 4:45 PM Tuesday (made the deadline)
- ATM network: 100% operational as of 11:00 PM Tuesday
- Data integrity issue: Resolved using Option B (manual correction of affected accounts completed overnight)
- Vendor licensing: Resolved after CIO escalation to FiServ executive leadership

Current Situation:

- The bank has been operating from the DR site for 26 hours successfully
- No customer data loss
- No regulatory violations
- Customer complaints have decreased significantly
- Media coverage has been neutral to positive (focusing on quick recovery)

New Challenge: Return to Primary Site

The Chicago data center facility manager reports:

- Water has been removed, and the facility is drying out
- Damaged equipment has been identified and replacement orders placed
- Estimated timeline for primary site restoration: 5-7 days
- Insurance will cover equipment replacement but not business interruption costs

Decision Required:

- Continue operating from DR site until primary site is fully restored (5-7 days)
- Begin planning return to primary site
- Consider making the DR site the new primary (long-term operational change)

Additional Considerations:

- Operating from the DR site costs $50,000 per day in additional expenses
- Staff are working split between Chicago and Milwaukee (travel and logistics challenges)

- Some staff have expressed concerns about returning to the Chicago facility
- Board of Directors wants a briefing on the incident and lessons learned

Your Response - Phase 4 (Due: Within 8 hours of Phase 3)

Task 4.1: Transition Planning (10 points)

21 **Return Strategy:** Develop a strategy for transitioning back to normal operations. Should you:
   - ✓ Return to the Chicago primary site once restored?
   - ✓ Continue at DR site indefinitely?
   - ✓ Implement a hybrid approach?

22 Justify your recommendation with cost-benefit analysis and risk assessment.

23 **Transition Timeline:** Create a detailed timeline for your chosen transition approach including:
   - ✓ Key milestones and activities
   - ✓ Testing and validation requirements
   - ✓ Cutover procedures
   - ✓ Rollback plan if transition fails

24 **Business Resumption:** What steps will you take to fully resume normal business operations? Address:
   - ✓ Customer notification and confidence rebuilding
   - ✓ Staff return to normal schedules
   - ✓ Vendor and partner communications
   - ✓ Regulatory close-out

Final Deliverable: Comprehensive After-Action Report (Due: End of Week 21)

Task 5.1: After-Action Report (AAR) (15 points)

Prepare a comprehensive After-Action Report documenting the entire disaster recovery operation. Your AAR must include:

1. Executive Summary (1-2 pages)

- Incident overview and timeline
- Recovery actions taken
- Final outcome and business impact
- Key lessons learned
- High-level recommendations

2. Incident Timeline (2-3 pages)

- Detailed chronological timeline of the incident from initial event through recovery completion

- Key decisions and actions at each phase
- System restoration milestones
- Stakeholder communications

3. Recovery Performance Analysis (3-4 pages)

- Actual vs. target RTO/RPO for each system
- Analysis of what went well
- Analysis of what didn't go well
- Root cause analysis of complications and delays
- Resource utilization and efficiency

4. Decision Analysis (2-3 pages)

- Review of major decisions made during the incident
- Justification for decisions in hindsight
- Alternative options considered
- Lessons learned from decision-making process

5. Stakeholder Management Review (2 pages)

- Effectiveness of communications
- Stakeholder satisfaction assessment
- Media and public relations outcomes
- Regulatory compliance and reporting

6. Financial Impact Assessment (1-2 pages)

- Direct costs (DR site operation, equipment replacement, overtime)
- Indirect costs (lost revenue, customer attrition, productivity loss)
- Insurance recovery
- Total cost of disaster

7. Lessons Learned (2-3 pages)

- What worked well and should be reinforced
- What didn't work and needs improvement
- Gaps in DR plan, procedures, or capabilities
- Training and preparedness issues identified
- Technology or infrastructure improvements needed

8. Recommendations and Action Plan (2-3 pages)

- Specific recommendations for improving BC/DR capabilities
- Prioritized action plan with owners and timelines
- Resource requirements for improvements

- Metrics for measuring improvement

9. Appendices

- Communications sent during incident (executive updates, regulatory notifications, customer messages)
- Recovery timeline diagrams
- Resource allocation matrices
- Risk registers
- Decision logs

Submission Requirements

Format and Structure

Your submission must include:

25 **Phase Responses:** Individual responses to each phase (Tasks 1.1, 2.1, 2.2, 3.1, 3.2, 4.1) submitted as you complete each phase

26 **Final After-Action Report:** Comprehensive AAR (Task 5.1) submitted at the end

Technical Requirements

- Professional business document format
- Executive-level writing appropriate for board presentation
- Use tables, timelines, and diagrams to present information clearly
- Proper grammar, spelling, and professional tone
- Page numbers and headers/footers
- Citations for any external sources or frameworks referenced

File Submission

Phase Responses:

- Submit each phase response as completed (don't wait until the end)
- Format:PDF

Final After-Action Report:

- Format: PDF
- Length: 15-25 pages (excluding appendices)

Submit all files through the course learning management system by the due date.

Professional Quality Deductions

- Poor formatting, grammar, or spelling: -5 points
- Late phase submission: -3 points per phase per day
- Late AAR submission: -10 points per day (up to 3 days)
- Missing required sections: -5 points per section
- Inadequate length: -10 points
- Unrealistic or impractical responses: -5 to -15 points

Learning Objectives

Upon successful completion of this simulation, you will be able to:

27 Execute disaster recovery procedures under realistic time pressure and constraints
28 Make critical decisions, balancing competing priorities and incomplete information
29 Coordinate cross-functional recovery teams and allocate resources effectively
30 Manage stakeholder communications during crises
31 Apply RTO/RPO concepts to real-world recovery prioritization
32 Conduct after-action analysis and develop actionable improvement recommendations
33 Demonstrate practical BC/DR leadership and decision-making skills

Tips for Success

34 **Think Realistically:** This is a simulation of a real disaster. Your decisions should be practical and executable, not theoretical or idealistic.
35 **Manage Time Pressure:** In real disasters, you must make decisions with incomplete information. Don't wait for perfect information; make the best decision you can with what you have.
36 **Balance Competing Priorities:** You can't do everything at once. Prioritize based on business impact and make trade-offs explicitly.
37 **Communicate Effectively:** Tailor your communications to each audience. Executives need different information than technical teams or customers.
38 **Document Your Reasoning:** Explain why you made each decision. Your justification is as important as the decision itself.
39 **Learn from Complications:** The complications are designed to test your problem-solving. Show creativity and resilience in addressing challenges.
40 **Be Professional:** Write as if your responses will be reviewed by the CEO, board of directors, and regulators. Maintain professional tone and quality throughout.
41 **Use the AAR Effectively:** The After-Action Report is your opportunity to demonstrate learning and improvement. Be honest about what didn't work and provide actionable recommendations.

Frequently Asked Questions

Q: Can I make assumptions not stated in the scenario?
A: Yes, but document your assumptions clearly. Make reasonable assumptions consistent with the scenario. Avoid assumptions that fundamentally change the situation.

Q: What if I make a "wrong" decision?
A: There are often no perfect answers in disaster recovery. You're graded on your reasoning and justification, not on making the "right" choice. Defend your decisions with sound analysis.

Q: How detailed should my communications be?
A: Communications should be realistic, similar to what you would actually send in a real incident. Be clear, concise, and appropriate for the audience.

Q: Can I consult external resources during the simulation?
A: Yes, you may reference DR frameworks, best practices, and industry standards. This simulates having access to resources during a real incident.

Q: What if I can't complete a phase in the suggested timeframe?
A: The timeframes are guidelines. Quality is more important than speed. However, demonstrate that you understand the time pressure inherent in real disasters.

Q: Should I include actual technical commands in recovery procedures?
A: Focus on strategic and tactical decisions rather than specific technical commands. Show you understand the recovery process without getting lost in technical details.

Academic Integrity

This is an individual assignment. While disaster recovery is typically a team effort, this simulation tests your individual decision-making and leadership capabilities. All work must be your own.

You may reference frameworks, standards, and best practices, but all decisions, communications, and analyses must be original. Collaboration with classmates on specific scenario responses constitutes academic dishonesty.

This simulation will challenge you to apply BC/DR knowledge under realistic pressure. Approach it seriously, think critically, and demonstrate the leadership and decision-making skills required of effective disaster recovery managers. Good luck!