DECEMBER 17, 2025

AFTER-ACTION REPORT

FINAL DELIVERABLE

OLUWATIMILEHIN OLUWAGBEMI
FINANCEFIRST

Table of Contents

Executive Summary

Incident Overview

Due to floods brought on by a water main break on the street, FinanceFirst Bank's main data center in Chicago was severely disrupted on Tuesday at 6:30 AM CT. All production systems, including core banking, online and mobile banking, ATMs, and wire transfer processing, were rendered completely inoperable when water seeped onto the data center floor, necessitating an urgent power shutdown. Branch operations were set to begin in two hours, potentially impacting almost 250,000 clients in five states.

Due to the incident's Priority 1 classification, the bank's Disaster Recovery (DR) plan was activated. The primary data center suffered catastrophic physical damage, according to an early assessment, necessitating the activation of the Milwaukee DR site and collaboration with internal teams, executives, and regulatory authorities.

Recovery Actions Taken

The bank’s response followed a structured, phased approach:

1. **DR Activation (Phase 1):** The DR site was activated minutes after the incident. Executive and regulatory notices were sent out, and critical personnel were mobilized. In order to control expectations, communications with clients and branch managers started right away.
2. **Recovery Execution (Phase 2):** Priority was given to core banking systems, branch teller systems, wire transfer processing, and ATM network repair. To expedite time-sensitive procedures, such as pending wire transactions totaling $23.5 million, parallel recovery streams were set up. Manual online banking system configuration, personnel delays due to traffic, and media attention were among the difficulties.
3. **Complications Management (Phase 3):** The recovery team faced several unexpected issues:
    - Data corruption affecting 2,000 customer accounts in the latest backup
    - Wire transfer deadlines with only three hours remaining
    - Vendor licensing constraints preventing extended DR operation without escalation
    - Staff fatigue impacting operational efficiency
      Decisions were made to manually correct affected accounts (Option B), execute parallel wire transfer recovery, escalate vendor licensing issues to executive leadership, and rotate staff to manage fatigue.
4. **Stabilization and Transition Planning (Phase 4):** The DR site's core banking system was up and running by 5:30 PM on Tuesday. By 11:00 PM, all customer-facing services had been restored, the wire transfer deadline had been fulfilled,

and ATMs were completely functional. Overnight, problems with data integrity were fixed, guaranteeing that no client data was lost. While the Chicago primary data center underwent evaluation and equipment replacement, the DR site continued to serve as the operational hub.

5. **Final Outcome and Business Impact**

- Customer Impact: Minimal; only 2,000 accounts required manual adjustment, representing <1% of total customers. Communication mitigated frustration.
- Regulatory Compliance: All notifications and reporting obligations were met; no violations occurred.
- Operational Impact: All critical systems restored within the same business day; the DR site successfully supported operations for 26 continuous hours.
- Reputational Impact: Media coverage remained neutral-to-positive, emphasizing the bank's rapid recovery. Customer confidence improved with transparent communications.
- Financial Impact: Direct DR costs amounted to $350,000, plus overtime of $120,000. Indirect costs were minimal. Equipment replacement costs were covered by insurance.

Key Lessons Learned

- **DR Documentation Gaps:** Incomplete runbooks and undocumented manual procedures caused delays in online banking restoration.
- **Vendor Dependencies:** Licensing constraints highlighted the need for pre-negotiated DR arrangements with vendors.
- **Staff Management:** Prolonged recovery periods require structured shift rotations to reduce fatigue and human error.
- **Physical Risk Mitigation:** Primary data center flood vulnerability must be addressed to prevent future incidents.
- **Parallel Execution and Decision-Making:** The ability to execute critical operations in parallel significantly reduced operational risk and preserved compliance.

High-Level Recommendations

1. **Enhance DR Documentation:** Ensure all manual configurations and system recovery procedures are fully documented.
2. **Increase DR Testing Frequency:** Semi-annual full DR exercises to test readiness under realistic conditions.
3. **Strengthen Vendor Contracts:** Include explicit DR licensing support clauses.

4. **Automate Key Recovery Steps:** Reduce manual intervention for online and mobile banking systems.
5. **Improve Physical Resilience:** Implement flood prevention measures at the primary data center.
6. **Staff Fatigue Mitigation:** Implement formal shift rotations and on-call backup protocols for extended recovery operations.
7. **Executive & Regulatory Engagement:** Maintain proactive, transparent communication channels during high-impact incidents.

Incident Timeline

Phase 1: Incident occurrence and Declaration – Tuesday, 6:30 AM – 9:00 AM CT

6:30 AM – Incident occurrence

The basement of the Chicago central data center quickly flooded due to a municipal water main breakdown outside. The data center was on the first floor, which was flooded. Facility management promptly turned off all production systems as part of a complete power shutdown as a safety measure.

6:45 AM – Incident declaration and assessment

The Night Operations Manager notified the Disaster Recovery Manager of:

- Standing water (4–6 inches) in the data center
- Complete loss of power
- Inaccessibility of the facility
- Unknown extent of hardware damage

The incident was classified as Priority 1 / Severity 1 due to total system outage and physical infrastructure compromise.

6:50 AM – Safety and Personnel Accountability

Immediate confirmation was obtained that:

- No injuries occurred
- All on-site staff were safely evacuated
- Access to the facility was restricted for safety reasons

Personnel safety was documented as the priority.

7:00 AM – Disaster Recovery Plan Activation

Based on the severity, uncertainty of restoration timelines, and multiple RTO breaches, the full Disaster Recovery (DR) Plan was formally activated. The Milwaukee DR site was designated as the operational recovery location.

7:05 AM – Incident command structure established

The position of Incident Response Manager was taken over by the Disaster Recovery Manager. To provide traceability and regulatory defensibility, an event record, decision log, and communication cadence were built.

7:15 AM – Executive Notification

Executive leadership (CEO, CFO, CIO, COO) was notified of:

- Nature and cause of the incident

- Immediate business impact
- Decision to activate DR
- Initial recovery priorities

Executive sponsorship and support were confirmed.

8:00 AM – Regulatory Notification Initiated

Initial notifications were prepared and submitted to the Federal Reserve/FDIC within required timeframes, disclosing:

- Cause of disruption
- Scope of impact
- DR activation status
- Commitment to ongoing updates

9:00 AM – Transition to Recovery Execution

DR teams were fully mobilized at the Milwaukee site. Network connectivity and backup availability were validated, marking the transition from incident response to recovery execution.

Phase 2: Recovery Execution and Escalation – Tuesday, 9:00 AM – 12:00 PM CT

9:00 AM – Core System Recovery Initiated

Recovery efforts began with core banking systems, recognizing their foundational dependency for teller, ATM, wire, and online services. Parallel preparation began for branch teller systems.

9:30 AM – Recovery Delays Identified

Initial estimates indicated that core banking restoration would exceed the 4-hour RTO due to:

- Data validation complexity
- Infrastructure configuration steps

The revised timeline was escalated to executive leadership.

10:00 AM – Branch and Customer Pressure Escalation

Branch managers reported increasing customer frustration. Call center volumes rose to 300% of normal levels, and customers began posting complaints on social media.

10:30 AM – Media Attention

Local media outlets reported on the outage, increasing reputational risk. Communications teams coordinated messaging to ensure accuracy and consistency.

12:30 PM – Branch Teller System Restored

Branch teller systems were successfully restored at the DR site, enabling in-branch transactions to resume, significantly reducing customer impact at physical locations.

Phase 3: Complications and Critical Decision-Making – Tuesday, 2:00 PM – 6:00 PM

2:00 PM – Review of recovery status

At this point:

- Core banking was 80% restored
- Online and mobile banking had limited functionality
- The ATM network was partially operational
- The wire transfer system had not yet been restored

This prompted a reassessment of priorities.

2:05 PM – A Data Integrity Issue was discovered

The database team identified corruption in the most recent backup (6:15 AM), affecting approximately 2,000 customer accounts. Three remediation options were evaluated, each with regulatory, operational, and reputational implications.

2:30 PM – Decision was made on the Data Integrity Issue

Leadership approved Option B: use the latest backup and manually correct affected accounts. This decision preserved transaction continuity for the majority of customers while allowing targeted remediation.

2:45 PM – Wire Transfer Deadline Risk

With only three hours remaining before the 5:00 PM cutoff, a parallel recovery stream was initiated to restore the wire transfer system without halting core banking progress.

3:00 PM – Vendor Licensing Escalation

The core banking vendor required a special license for extended DR operation. After unsuccessful standard escalation, the issue was elevated to executive leadership, resulting in direct CIO-to-vendor executive engagement.

4:45 – Wire Transfers Deadline met

All 47 pending wire transfers totalling $23.5 million were processed successfully before the cutoff, avoiding contractual penalties and regulatory scrutiny.

5:30 PM – Core Banking System fully operational

The core banking system was declared fully operational at the DR site. This marked the formal completion of critical recovery objectives.

Phase 4: Stabilization and Transition – Tuesday Evening – Wednesday, 8:00 AM CT

Tuesday Evening – ATM and Data Remediation Completion, Vendor Licensing Resolution

ATM network reached 100% operational status by 11:00 PM

- Manual correction of affected customer accounts was completed overnight
- No residual data integrity issues were detected

Following executive escalation, the vendor provided the required licensing authorization, ensuring uninterrupted DR operations beyond 24 hours.

Wednesday, 8:00 AM – Operation becomes stabilized

By Wednesday morning:

- All systems were fully operational
- The bank had operated successfully from the DR site for 26 hours
- Customer complaints had significantly decreased
- Media coverage shifted to positive recovery narratives
- No regulatory violations were recorded

In Summary, the incident lifecycle—from disruption to stabilized operations was managed within regulatory expectations through:

- Rapid activation of the DR plan/site
- Disciplined decision-making
- Parallel recovery execution
- Effective stakeholder communication

The timeline demonstrates organizational resilience, governance maturity, and operational control under crisis conditions.

Recovery Performance Analysis

Actual vs. Target RTO and RPO

The bank's predetermined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for important systems were used to gauge the disaster recovery performance. Overall, recovery goals were mostly achieved, with a few small deviations caused by choices on resource prioritizing and data integrity.

System	Target RTO	Actual RTO	Target RPO	Actual RPO	Performance Assessment
Core Banking System	12 hours	11 hours	30 minutes	0-30 minutes	Met
Online Banking	8 hours	7 hours	15 minutes	15 minutes	Met
Mobile Banking	8 hours	7.25 hours	15 minutes	15 minutes	Met
Branch Teller System	6 hours	5.75 hours	15 minutes	15 minutes	Met
ATM Network	24 hours	16.5 hours	30 minutes	30 minutes	Exceeded
Wire Transfer System	10 hours	9.5 hours	Zero data loss	Zero data loss	Met

Analysis:

- RTO targets were achieved for all Tier-1 systems despite infrastructure damage at the primary data center.
- RPO objectives were maintained through disciplined backup management and the decision to manually correct corrupted records rather than reverting to older backups.
- The ATM network recovery exceeded expectations due to partial restoration strategies and staggered testing.

What went well?

Several aspects of the recovery demonstrated strong disaster recovery maturity:

1. **Timely DR Plan Activation:** The incident was quickly identified as critical, enabling rapid decision-making, leading to early activation of the DR plan, preventing prolonged system outage and uncontrolled recovery efforts.
2. **Effective Command and Control:** a centralized incident command structure that ensured clear authority, rapid escalation, consistent status reporting, and decision logs were maintained throughout the incident, supporting accountability
3. **Prioritization of Customer-Oriented Systems:** the restoration sequence focused majorly on branch teller systems, digital banking channels such as

online banking portal, mobile app, and wire transfer system. This minimized customer data disruption and prevented contractual breaches.

4. **Regulatory and Stakeholder Communication:** The Federal Reserve/FDIC were notified accurately and on time to reduce regulatory risk and reputational damage.
5. **Vendor Escalation Success:** The CIO escalation to the FiServ CEO resolved the licensing risk before the system shutdown

What did not go well?

Despite overall success, several challenges were identified:

1. Backup Integrity Validation Gaps: The corruption in the most recent backup was not detected until restoration was underway. The pre-incident backup verification processes were not sufficient.
2. Wire Transfer System De-Prioritization: Initial focus on core banking delayed wire transfer restoration. The compressed recovery window increased operational stress and risk.
3. Staff Fatigue and Human Error Risk: due to extension in the work hours, there were minor configuration errors, slower decision cycles, and backup staff were not familiar with DR procedures, limiting immediate relief.
4. Vendor Dependency Risk: Licensing constraints were not fully accounted for in DR planning. Over-reliance on a single vendor escalation path increased exposure.

Root cause analysis of complications

Complication	Root Cause	Contributing Factor
Backup Corruption	Inadequate Integrity Checks	Limited automated validation
Wire Transfer Delay	Resource Prioritization	Underestimated system criticality
Licensing Risk	Contractual Oversight	DR Licensing terms are not explicit
Staff Fatigue	Prolonged recovery window	Insufficient rotation planning

Summary: Most issues were governance and process-related rather than technological. This suggests that infrastructural expenditures were successful, but there is room for development in procedural maturity.

Resource Utilization and Efficiency

Human Resources

- Core DR staff operated continuously for 8–12 hours.
- Backup staff availability was adequate but underutilized initially.
- Decision-making slowed as fatigue increased.

Technical Resources

- DR site capacity proved sufficient for full operational load.
- Network and storage performance met expectations.
- Parallel recovery capability was present but not fully leveraged.

Financial Resources

- DR site operational cost: $50,000/day
- Overtime and travel expenses increased total recovery cost.
- Early stabilization reduced long-term financial exposure.

Efficiency Assessment:

Resource utilization was effective but not optimized, particularly regarding staff rotation and parallel system recovery.

Overall Performance Rating

Area	Rating
RTO/RPO Achievement	Excellent
Incident Command	Strong
Technical Recovery	Strong
Data Management	Moderate
Vendor Management	Moderate
Staff Sustainability	Needs Improvement

Decision Analysis

All major decisions during the incident were made using a risk-based, business-impact-driven framework, informed by:

- Predefined RTO/RPO values from the Business Impact Analysis (BIA)
- Regulatory obligations (Federal Reserve, FDIC, GLBA)
- Customer and reputational risk considerations
- Available technical and human resources
- Time-critical business deadlines (e.g., wire transfer cutoff)

Decision authority followed the documented incident command structure, with escalation to executive leadership where business risk exceeded predefined thresholds.

Decision 1 - Activation of the Disaster Recovery Plan: The major data center was inaccessible owing to flooding that caused a power loss, thus it was decided to activate the full disaster recovery plan. All Tier 1 system RTOs were exceeded by the projected time for recovering the major data center. NIST SP 800-34 CP-10 states that when system availability cannot be restored in a reasonable amount of time, recovery must be started. When disruption criteria are exceeded, ISO 22301 Clause 8.4.1 requires continuity measures to be carried out.

Alternatives Considered

Options	Assessment
Wait for primary site restoration	Rejected – unacceptable RTO breach
Partial DR activation	Rejected – interdependencies between systems
Full DR activation	Selected – lowest business and regulatory risk

Decision 2 - System Recovery Prioritization: The decision was to recover the system in the following order:

- Branch Teller System
- Core Banking System
- Online & Mobile Banking
- ATM Network
- Wire Transfer System (parallelized later)

All transaction processing is supported by branch operations and core banking, which is why that arrangement was chosen. Downstream client services require tellers and core systems. At first, wire transactions were given less priority, but as the deadline drew near, they were reevaluated. Clause 8.3.2 of ISO 22301 states that continuity plans must be in line with activities that are given priority. Among the lessons learned

are: Time pressure rose when wire transfers were initially deprioritized; Time-bound regulatory transactions should be specifically noted in future planning.

Decision 3 - Data Integrity Resolution Strategy

Decision 3 - Option B: Use the most recent backup and manually correct affected accounts: this decision preserved RPO commitment, avoided customer financial discrepancies, supported the GLBA data integrity requirements, and also aligned with ISO 22301 Clause 8.4.3.

Options Analysis

Option	Risk	Impact	Regulatory Consideration
A – Older Backup	Data Loss	High customer impact	Regulatory concern
B – Manual Correction	Resource Intensive	No data loss	Compliant
C – Delay Recovery	Unknown downtime	Severe Impact	Unacceptable

Decision 4 - Initiate parallel recovery of the wire transfer system while continuing core banking restoration: Missing the deadline for wire payments could have resulted in a contract violation, financial harm to the consumer, and regulatory attention. Analyzing the Risk-Benefit, we averted significant regulatory and reputational harm in accordance with ISO 22301 Clause 8.4.2, which manages competing recovery priorities, even though the choice would cause core banking to be delayed owing to resource diversion.

Decision 5 - Vendor Licensing Escalation by escalating the licensing issue to executive and vendor senior leadership. Vendor dependence is outside of internal technical control, and license expiration puts DR continuity at risk. In order to obtain a temporary extension, the CIO had to include FiServ executive leadership in legal and vendor management team interaction. This choice complies with ISO 22301 Clause 8.4.4: Assurance of Supplier Continuity. Lessons Learned include:

- DR licensing must be contractually guaranteed.
- **Vendor escalation paths should be pre-documented.**

Decision 6 - Staff Fatigue and Resource Management: shift rotation was implemented, and backup staff was introduced with oversight because prolonged cognitive fatigue will increase error rates. This decision led to a reduced error rate overnight, maintained recovery momentum also identified the need for broader DR cross-training.

Lessons Learned from all the decisions made:

- Time-based regulatory obligations must be elevated in prioritization models
- Data integrity preservation outweighs short-term recovery speed
- Vendor dependencies are critical DR risk factors.
- Human resilience is as important as technical resilience
- Pre-authorization and documentation reduce crisis decision friction

The FinanceFirst Bank disaster recovery event's decision-making process, which was marked by prompt escalation, risk-based prioritization, and regulatory awareness, showed high agreement with NIST SP 800-34 and ISO 22301. Even though a number of decisions were made under tremendous time pressure, the results show a developed governance structure with obvious room for contractual and procedural improvements.

Stakeholder Management Review

A key component of FinanceFirst Bank's disaster recovery operation's success was effective stakeholder management. The event required prompt, accurate, and role-appropriate communication with internal and external stakeholders due to its high visibility, regulatory supervision, and direct customer effect.

The bank followed a structured communication hierarchy defined in the Disaster Recovery and Business Continuity Plans, ensuring that:

- Information was consistent and factual
- Communications were tailored to stakeholder needs
- Regulatory notification timelines were met
- Reputational risk was actively managed
- 2 Executive Leadership Communication

Communication Effectiveness

- Executives were notified within 30 minutes of DR plan activation.
- Hourly situation updates were provided during critical recovery windows.
- Communications included:
    - Current system status
    - Key risks and constraints
    - Revised recovery timelines
    - Mitigation actions and decision points

Assessment

- Executive leadership expressed confidence in the recovery process.
- Early transparency enabled rapid escalation (e.g., vendor licensing issue).
- Communication supported informed decision-making, consistent with ISO 22301 Clause 7.4.2.

Areas for Improvement

- Formal executive dashboards could further enhance real-time situational awareness.
- Pre-approved decision thresholds should be more explicitly documented.

Regulatory Communication and Compliance Reporting (Federal Reserve/Federal Deposit Insurance Corporation (FDIC))

Actions Taken

- Initial regulatory notification sent within 4 hours, meeting statutory requirements.
- Follow-up reports documented:

- Nature and cause of the incident
- Systems affected
- Data integrity status
- Recovery actions and timelines
- Ongoing updates were provided until full-service restoration.

Assessment

- No regulatory violations or enforcement actions resulted.
- Regulators acknowledged timely and comprehensive communication.

Areas for Improvement

- Standardized regulatory reporting templates could reduce preparation time.
- A centralized regulatory contact matrix should be maintained and tested.

Media and Public Relations Management (Local and regional news outlets, General public)

Actions Taken

- Issued a controlled media statement acknowledging the incident.
- Emphasized customer protection, safety, and recovery progress.
- Avoided speculative or technical detail that could cause alarm.

Assessment

- Media coverage remained neutral to positive.
- No misinformation or reputational escalation occurred.
- Demonstrated alignment with ISO 22301 Clause 7.4.3 regarding external communication control.

Stakeholder Satisfaction Assessment

Stakeholder Group	Satisfaction Level	Evidence
Executive Leadership	High	Continued support, rapid escalation
Regulators	High	No findings or penalties
Customers	Medium – High	Compliant decline, retention preserved
Branch Staff	Medium	Initial uncertainty improved over time
Media / Public	High	Neutral to Positive coverage

During the disaster recovery occurrence, FinanceFirst Bank's stakeholder management was efficient, prompt, and compliant with ISO 22301 and NIST SP 800-34 standards. A controlled recovery was made possible by effective executive and regulatory communication, and reputational harm was lessened by customer-focused messaging.

Financial Impact Assessment

The Financial Impact Assessment assesses the direct, indirect, and residual financial effects of FinanceFirst Bank's primary data center outage and the ensuing disaster recovery efforts. The Business Continuity and Disaster Recovery (BC/DR) program's ongoing improvement, insurance claims, executive control, and regulatory transparency are all supported by this evaluation. Documented recovery operations, actual operating expenses, expected revenue, productivity implications, insurance coverage restrictions, and cost avoidance through timely recovery are all included in the assessment.

Direct Costs

Disaster Recovery Site Operating Costs: The DR site costs $50,000 per day for daily operations. The mid-incident through primary site readiness lasted for 6 days, and the total DR site cost is $300,000

Equipment Replacement and Facility Restoration, such as water-damaged servers, storage arrays, and network equipment, environmental remediation and facility drying, replacement lead times of 5–7 days are estimated to cost $1.4 million

Overtime and Staffing Costs: extended work hours for IT, security, facilities, call center, and branch staff, manual data reconciliation for 2,000 customer accounts, shift rotations, and fatigue mitigation measures are estimated to cost $180,000

Total Direct Cost

Cost Category	Amount
DR Site Operations	$300,000
Equipment Replacement	$1,400,000
Overtime & Staffing	$180,000
Total Direct Costs	$1,880,000

Indirect Costs

Lost or Deferred Revenue: Temporary inability to process certain transactions, delays in loan origination and approvals, reduced transaction volumes during outage windows estimated Impact is $450,000

Productivity Loss: Reduced staff efficiency due to system downtime, manual processing, and workarounds, executive and management time diverted to incident management, estimated Impact is $220,000

Customer Attrition and Relationship Risk: Increased customer dissatisfaction during outage, threatened account closures reported by branch managers, and potential long-term impact on customer lifetime value estimated. Impact is $300,000.

Total Indirect Costs

Category	Amount
Lost/Deferred Revenue	$450,000
Productivity Loss	$220,000
Customer Attrition Risk	$300,000
Total Indirect Costs	$970,000

Insurance Coverage: Physical equipment damage and facility restoration are covered by insurance, while business interruption and DR operational expenses are not covered by insurance

Insurance Recovery: The expected reimbursement by insurance is about $1.4M with pending claim settlement.

DR operational costs and lost revenue were not insured, which identifies a gap in the current insurance coverage strategy

Total Cost of the Disaster

Cost Category	Amount
Total Direct Costs	$1,880,000
Total Indirect Costs	$970,000
Gross Impact	$2,850,000
Less: Insurance Recovery	$1,400,000
Net Financial Impact	$1,450,000

Lesson Learned

The FinanceFirst Bank disaster recovery incident provided a real-world stress test of the organization's Business Continuity and Disaster Recovery (BC/DR) capabilities. While recovery objectives were largely met, the incident revealed both **strengths to be reinforced and gaps requiring remediation.

This section documents key lessons learned across governance, technology, people, processes, and third-party dependencies, in line with the continuous improvement requirements of:

- NIST SP 800-34 (CP-4, CP-10)
- ISO 22301:2019 Clause 10 (Improvement)

What Worked Well and Should Be Reinforced:

- **Early and Decisive DR Plan Activation:** the lesson learnt from this decision is that rapid activation of the DR plan prevented prolonged outages and regulatory breaches. The DR plan was activated minutes after the confirmation of the incident, leading to the restoration of systems within approved RTOs, no record of data loss, and no regulatory violations. This procedure aligns with ISO 22301 Clause 8.4 (Effective continuity procedures). The actions needed to make this more effective include the maintenance of low activation thresholds and empowering DR leadership to act without delay.
- **Warm Site Strategy Effectiveness**: the warm site provided a viable and reliable recovery environment, the infrastructure became operational upon activation, network and access controls functioned as designed, and it also supported full restoration of customer service. The actions needed to make this more effective include continuous investment in warm-site readiness and increased automation to reduce manual configuration.
- **Strong Executive and Regulatory Engagement:** There is transparent and timely communication with executives and regulators, which reduces risk and uncertainty. Regulators were notified within required timelines; executive support enabled fast escalation; no regulatory findings or penalties. The actions needed to make this more effective include preserving structured executive briefing cadence and formalizing regulator communication templates.
- **Customer Trust Preservation Through Communication:** There is proactively mitigated reputational damage through customer complaints peaking early, due to concise communication, which declined quickly, retaining high-value customers, and media coverage was neutral. The action needed to make this effective is to expand automated customer notification capabilities.

What Did Not Work Well and Needs Improvement:

- **Backup Integrity Validation Gaps:** Backups were available but not fully validated for integrity before restoration. Data corruption was discovered post-recovery initiation, with the option to reconcile with losing 2,000 accounts. The action needed to curb this is to implement automated backup integrity checks and introduce pre-restore validation procedures.
- **Incomplete DR Documentation:** Manual configuration steps were insufficiently documented. This led to a delay in restoring the online banking portal. There is a need to update DR runbooks with step-by-step procedures, conduct peer reviews of documentation.
- **Staff Fatigue and Knowledge Concentration:** Extended work periods increased error risk and stress. Minor operational errors were observed due to heavy reliance on key technical staff. It is required to introduce mandatory shift rotation plans and expand DR cross-training programs.
- **Vendor Dependency Risks:** Vendor licensing constraints posed a critical continuity risk. There was a potential system shutdown without license renewal; the had to be executive escalation before it was resolved. There is a need to update contracts to include DR licensing clauses and maintain vendor escalation matrices.

Technology and Infrastructure Lessons

- Real-time replication significantly reduced data loss risk
- Manual recovery steps increased recovery time variability
- Centralized monitoring improved situational awareness

Improvement needed

- Increase automation in DR failover processes
- Review the feasibility of active-active architectures for Tier-1 systems

Training and Preparedness Lessons

- Tabletop exercises were beneficial but insufficient
- Last full DR test was 18 months prior

Improvement needed

- Conduct annual full-scale DR tests
- Increase scenario complexity (e.g., data corruption, vendor failure)

Gaps in the DR plan, procedures, or capabilities

- Risk assessments did not fully account for the following:
    - Vendor licensing constraints
    - Extended DR operations costs
    - Staff endurance limits

Improvement needed

- Update enterprise risk register
- Incorporate financial and human resilience risks into BIA

Summary of Key Lessons Learned

Area	Key Lesson
Strategy	Early DR activation reduces overall risk
Technology	Backup integrity validation is critical
People	Human resilience planning is essential
Process	Documentation must support execution under stress
Vendors	Supplier dependencies require contractual assurance
Governance	Continuous improvement must be evidence-driven

Strong core BC/DR capabilities were demonstrated in the FinanceFirst Bank disaster recovery incident, and the results satisfied operational, customer, and regulatory requirements. The lessons learnt show that procedural and governance issues, rather than design flaws, accounted for the majority of defects.
The bank can move from a compliant BC/DR posture to a high-maturity, resilient operating model in accordance with the continuous improvement principles of ISO 22301 and NIST SP 800-34 by filling in the gaps that have been found.

Recommendation and Action Plan

The recommendations and action plan are derived directly from:

- Observed performance during the disaster recovery incident
- Identified gaps in technology, processes, people, and governance
- Requirements for continuous improvement under ISO 22301 Clause 10
- Control expectations defined in NIST SP 800-34

The objective is to enhance FinanceFirst Bank's resilience, recovery speed, data integrity, and stakeholder confidence, while ensuring ongoing regulatory compliance and cost efficiency.

Recommendations

- **Strengthen Backup Integrity and Data Resilience:** Implement automated backup validation and integrity checking across all Tier-1 and Tier-2 systems. This will:
    - Prevents recovery delays due to corrupted backups
    - Reduces reliance on manual data reconciliation
    - Protects customer data integrity
- **Enhance Disaster Recovery Automation:** Increase automation of failover, configuration, and restoration processes at the DR site. This will:
    - Reduces human error under stress
    - Improves consistency and predictability of recovery
    - Shortens actual RTOs
- **Improve DR Documentation and Runbooks:** Fully document all manual DR procedures with step-by-step runbooks and validation checklists. This will:
    - Reduces dependency on key individuals
    - Supports less experienced staff during recovery
    - Improves audit readiness
- **Strengthen Human Resilience and Staffing Models:** Implement formal shift-rotation plans and cross-training for DR-critical roles. This will:
    - Prevents staff fatigue and operational errors
    - Ensures continuity during extended incidents
    - Builds organizational resilience
- **Formalize Vendor and Third-Party Continuity Requirements:** Update vendor contracts to explicitly include disaster recovery licensing, escalation procedures, and continuity assurances. This will:
    - Reduces vendor-related recovery risk
    - Prevents emergency escalation scenarios
    - Ensures uninterrupted DR operations
- **Expand Business Interruption Insurance Coverage:** Review and expand insurance policies to include business interruption and extended DR operating costs. This will:

    - Mitigates financial exposure during prolonged incidents
    - Aligns financial resilience with operational resilience
- **Improve Communication and Customer Notification Capabilities**: Deploy automated customer and stakeholder notification systems (SMS, email, status pages). This will:
    - Reduces call center overload
    - Improves transparency and customer confidence
    - Supports consistent messaging

Prioritized Action Plan

Action Item	Owner	Priority	Timeline
Implement backup integrity validation tools	IT Ops	High	30-60 days
Automate DR failover for Tier-1 systems	Infrastructure	High	60-90 days
Update and test DR runbooks	DR Manager	High	30 days
Conduct DR cross-training	HR/IT	Medium	90 days
Revise vendor contracts for DR licensing	Legal	Medium	120 days
Expand insurance coverage	Finance/Risk	Medium	120 days
Deploy automated customer alerts	Communication	Medium	90 days
Schedule a full-scale DR test	Risk/IT	High	6 months

Resource Requirements

Human Resources	Technology	Financial Investment
Additional DR Training Budget	Backup Validation Software	Estimated incremental investment of $600,000 - $900,000
Temporary consulting support for automation	DR orchestration tools and communication automation platforms	Expected ROI through reduced recovery time, lower labour costs, and avoided revenue loss

Metrics for Measuring Improvement

Metric	Baseline	Target
Core Banking RTO	11 hours	≤ 8 hours
Backup integrity Errors	Reactive	Zero
DR Staff Coverage	Limited	Fully Cross-Trained
Vendor DR Readiness	Partial	Contractually Guaranteed
Customer Complaints	Elevated	≤ 10% spike

To improve FinanceFirst Bank's BC/DR maturity from effective to highly resilient, the recommended actions offer a clear, prioritized roadmap. The bank can drastically cut future recovery time, financial exposure, and operational risk while upholding strict regulatory compliance by addressing technology, people, process, and governance holistically.

Appendices

Appendix A - Communications sent during incident (executive updates, regulatory notifications, customer messages)

1. Executive Communication

To: Executive Leadership (Email Update)

Subject: CRITICAL UPDATE: Data Center Disaster Recovery - 9:30 AM Status

Status: The DR Plan is fully activated. The Recovery Team is mobilized in Milwaukee. Core Banking System restoration is in progress, but delayed.

Challenge: The Core Banking recovery is estimated at ~ 6 hours (instead of 4), moving the expected completion to 4:00 PM CT. Online Banking configuration issues are being addressed, causing further delay.

Revised Timeline: We expect to restore Branch Teller Systems by 12:00 PM and Core Banking by 4:00 PM. The 5:00 PM Wire Transfer deadline is a critical risk but remains a target.

Mitigation: Resources have been shifted to prioritize Core Banking and Wire Transfer. We are drafting a public statement and ramping up call center staffing to manage reputational risk and customer frustration.

2. Regulatory Communication

To: Federal Reserve and FDIC

Subject: Formal Notification of Significant Operational Disruption - FinanceFirst Bank

FinanceFirst Bank is formally notifying you of a significant operational disruption that began at 6:30 AM CT due to catastrophic flooding at our Primary Data Center in Chicago, IL. All production systems are currently offline.

- Action Taken: Full DR Plan activated at the Milwaukee Warm Site.
- System Impact: All customer systems affected (Online, Core, ATM).
- Recovery Status: Core Banking restoration is underway. We anticipate a revised recovery time of 4:00 PM CT for the Core System.
- Data Integrity: No data loss reported as of 6:15 AM replication.
- Compliance: We are prioritizing restoration of critical regulatory reporting systems and will continue to provide status updates every 4 hours until recovery is complete.

3. Customer Communication

Website banner alert

URGENT: We are experiencing a major system outage due to an incident at our main data center. Our teams are executing our Disaster Recovery plan. Online and Mobile Banking are temporarily unavailable. We apologize for the inconvenience and are working to restore service as soon as possible.

Social Media Post

We are aware of the system outage. We are actively working to restore services. Our branches are open for limited services (cash/check deposits/withdrawals). We appreciate your patience. Next update at 1:00 PM CT.

Branch Signage

SYSTEMS DOWN: Due to an unexpected incident, our computer systems are temporarily unavailable. We can only process limited transactions manually. Please expect delays. We are committed to restoring full service as quickly as possible.

Call Center Talking Points

"I understand your frustration. We experienced a major system outage this morning. Our specialized technical teams have activated our recovery site in Milwaukee and are working non-stop. We expect to have core services back online by 4:00 PM CT. Your funds are safe, and we will update our website immediately when service is restored."

4. Media management

Media Statement: FinanceFirst Bank confirms that an incident involving a municipal water main break caused a major outage at our primary Chicago data center this morning. We declared an emergency and successfully activated our Disaster Recovery plan. Our technical teams are working at our secondary location to restore all customer services. We apologize for the interruption and assure our customers that their funds and data remain safe.

5. Internal communication

Subject: INTERNAL: Important Update on System Outage and Customer Management

Status: We are operating under the full Disaster Recovery Plan. Branches are open but relying on manual processes. Core systems are expected back online around 4:00 PM CT.

Your Role: Your primary goal is to remain calm, professional, and empathetic. Use the Call Center Talking Points provided to manage customer expectations. DO NOT speculate on the cause or duration of the outage beyond the official guidance. Direct

all media inquiries to the Crisis Communications Team. Your support is crucial in maintaining customer confidence.

Appendix B – Risk Register

Risk Description	Probability	Impact	Mitigation Actions	Contingency Plan
Vendor License Expiration	High	High	Escalate to executive leadership; report to the CIO, while the CIO reports to the FiServ CEO. The legal team will review the contract.	If no response/key by midnight, the core banking system will be shut down and restarted.
Data Integrity remediation error	High	Medium	Senior QA will be assigned to lead the night shift to correct data errors manually	If the error persists, a full audit will be initiated, and the affected accounts will be isolated.
Wire Transfer Missing Deadline	High	High	Divert 2 staff to parallel recovery. Explore manual processing with a correspondent bank as a fallback.	If the deadline is missed, affected customers will be notified with a formal apology, also notify regulatory bodies.
Staff Fatigue/Burnout	High	Medium	Breaks will be mandated for staff; the shift will be initiated.	In case of an emergency, pull the staff off duty immediately and assign the task to the standby staff
ATM Instability	Medium	Medium	Implement a phased rollout	Disable unstable ATMs