Phase 1 (Due: Within 2 hours of the incident)

Task 1.1: Initial Assessment and Decision

1. **Situation Assessment**

After careful analysis of the situation, the severity of the incident is catastrophic. It led to the inaccessibility/disruption of the primary data center. If a data center is inaccessible, there will be business disruption, as all production systems are shut down due to a power outage.

The immediate business impact includes:

- Data Loss
- Unavailability of Retail and Commercial banking services
- Financial risk
- Reputation Damage
- Regulatory risk
- Operational risk

Information needed:

- Current status of IT equipment, whether it is a total loss/damage, or it can be worked on / restored at low cost
- Current status of environmental controls.
- What is the status of the DR site, whether it's a cold or warm site?
- What are the procedures available for recovery of affected systems?

2. **DR Plan Activation Decision**

My decision will be "YES," we need to activate the full disaster recovery plan. Considering the situation with the primary data center being flooded, restoring it will be impractical, and there's a need to save the day; business needs to continue, and customers are threatening to take business elsewhere, which will be very costly for the company. In order to meet critical RTOs, we need to activate the DR Plan. Though it might be costly, as long as it saves the business, the reputation is not damaged, and the company is not faced with a regulatory fine, it is preferable.

3. **Initial Actions (first 30 minutes)**

Specific actions:

- Formally declare the disaster
- Activation of the full DR Plan
- Commence incident log and timeline documentation

Who will I notify?

- Executive Leadership (CEO, CIO, COO, CCO)
- IT Team

Teams to mobilize:

- Core Incident Response Team
- Chicago IT staff
- Milwaukee IT staff
- Compliance team

Immediate steps:

- The compliance officer will prepare a notification to the regulatory bodies.
- Prioritize the first stage of system recovery, especially the Core Banking System.

4. **Communication Plan**

Executive Leadership

To: CEO, CIO, COO

Subject: P1 Incident – Chicago Data Center / DR Activation

At 6:30 AM CT, the Chicago data center experienced catastrophic flooding due to a city water main break. Power has been shut down, the facility is inaccessible, and all production systems are currently offline.

Based on the severity and expected restoration uncertainty, I am activating the full Disaster Recovery Plan and initiating failover to the Milwaukee DR site.

No injuries reported. Last successful data replication occurred at 6:15 AM.

We will prioritize core banking, teller systems, online/mobile banking, and wire transfer services.

The next executive update will be provided within 60 minutes.

Regulatory Notification

To: Federal Reserve and FDIC

Subject: P1 Incident – Chicago Data Center / DR Activation

FinanceFirst Bank is reporting a significant operational disruption.

At 6:30 AM CT on Tuesday, our primary data center in Chicago became unavailable due to flooding from a municipal water main failure, resulting in a full systems outage.

The bank has activated its Disaster Recovery Plan and is failing over critical banking systems to its designated DR site in Milwaukee.

No customer data loss is expected. Initial recovery efforts are underway, and further updates will be provided as the situation develops.

IT Recovery Team

To: IT and Operations

Subject: DR Event Declaration

The Chicago primary data center is offline due to flooding. The full DR plan is now active.

Milwaukee DR site teams: begin failover preparation immediately.

Priority order:

1. Core Banking
2. Branch Teller System
3. Online & Mobile Banking
4. Wire Transfer System

All actions must be logged. No changes without Incident Command approval.

Branch Managers

To: Branch Managers

Subject: DR Event Declaration

Due to an early-morning data center outage, all banking systems are currently unavailable.

Branches should open as scheduled, but **do not process transactions** until further notice.

Please reassure customers that systems are being restored via our disaster recovery facility.

We will provide updates every 60 minutes or sooner if service is restored.