

Disaster Recovery & Business Continuity Plan

FinSecure Bank - Financial Management System

Data Security, Governance and Compliance
Week 6: Planning for Contingencies

Group Members:

Janvi Poshia (2543705)
Sneha Bhesaniya (2544720)
Karina Jiwani (2536600)
Diyaben Patel (2532979)
Dharmikkumar Dabgar (2536691)

1. Analyse Your Scenario

Identify Potential Disasters

- **Cyberattacks:** Hackers trying to steal data or lock the systems (Ransomware).
- **Natural Disasters:** Floods, storms, or fires hitting the main data centre.
- **Man-Made Events:** An employee accidentally or purposely causing a data leak.
- **System Failures:** Major power cuts or internet outages stopping transactions.

Critical Business Functions & Assets

- **Core Banking System:** Needs to stay online for daily transactions and transfers.
- **Customer Data:** Must be kept secure with zero data lost.
- **Online Platform:** Essential for customers to access their accounts.
- **IT Hardware:** Servers and network equipment running the bank.

2. Designing the Business Continuity Plan (BCP)

Form the BC Team

- **BCP Coordinator:** Leads the team and makes final decisions.
- **IT Lead:** Focuses on keeping the servers and network running.
- **Communications Lead:** Tells staff and customers what is happening.
- **Operations Lead:** Makes sure manual banking can happen if computers are down.

Outline BC Strategies

- **Exclusive-Use (Hot Site):** The bank will have a mirrored, fully running backup data centre ready to go instantly.
- **Shared-Use (Warm Site):** Cloud backups for less urgent office work.
- **Specialised Options:** Using temporary remote-working setups for staff if the office is closed.

Develop the BC Policy

- **Purpose:** To keep FinSecure Bank running and protect customer money during a disaster.
- **Scope:** Includes all IT systems, staff, and bank branches.
- **Resource Requirements:** Backup servers, emergency funds, and emergency communication tools.
- **Roles:** Clear leadership structure during an emergency.
- **Training:** All staff get basic training; IT gets advanced recovery training.

Ensure Maintenance

- **Testing:** Doing practice runs (drills) every six months.
- **Periodic Updates:** Reviewing the plan every year or when a new system is added.

3. Designing the Disaster Recovery Plan (DRP)

Define Disaster Classifications

- **Natural (Rapid Onset):** Sudden events like fires or earthquakes.
- **Natural (Slow Onset):** Events with warning like approaching bad weather.
- **Man-Made:** Cyberattacks or system sabotage.

Outline Recovery Steps

- **Step 1:** Stop the problem (e.g., disconnect hacked servers).
- **Step 2:** Prioritise fixing the main banking systems first.
- **Step 3:** Switch traffic to the backup servers (Hot Site).
- **Step 4:** Check the data to make sure nothing was lost or changed.
- **Step 5:** Safely reopen access to customers.

Develop the DR Policy

- **Scope:** Focuses purely on fixing the IT systems and data.
- **Training:** Making sure IT knows how to use the backup servers.
- **Testing:** Checking backups every month to ensure they work.

Testing and Improvement

- **Simulations:** Practice "fake" cyberattacks to test response times.
- **Desk Checks:** Reading through the plan to check if contact numbers are correct.
- **Walkthroughs:** Team meetings to discuss step-by-step how they would handle an outage.