

Group member:

student id:

1) Dipkumar Patel

2535265

2) Devang Zala

2534443

3) Akash Luhariya

2535266

4) Yash Kachhadiya

2543707

FINSECURE BANK

Contingency Planning, Incident Response, & Business Continuity

This technical tutorial delivers an architectural overview of systems engineering and strategic policy operations designed to secure critical financial infrastructure for FinSecure Bank.

1. Foundations of Contingency Planning (CP)

In a modern, highly regulated digital banking ecosystem, a financial platform like FinSecure Bank cannot afford prolonged downtime or compromised data integrity. To guarantee systemic resilience, we implement a comprehensive Contingency Planning (CP) framework. This framework acts as an umbrella strategy that dynamically links three critical operational pillars:

- **Incident Response (IR):** Tactical, immediate actions designed to identify, contain, and neutralize an active security breach.
- **Business Continuity (BC):** Strategic operational plans ensuring key business operations continue to operate at minimal acceptable limits during an outage.
- **Disaster Recovery (DR):** Technical procedures and automated protocols to reconstruct or replicate failed IT infrastructure back to active operational baselines.

2. Incident Response (IR) Model (NIST SP 800-61 Rev. 2)

The tactical arm of our contingency strategy is governed by the National Institute of Standards and Technology (NIST) Incident Response lifecycle. This structured framework ensures that the Security Operations Center (SOC) can rapidly contain cyber threats through four distinct phases:

Phase 1: Preparation

Preparation forms the bedrock of FinSecure's defensive posture. This involves deploying automated WAF boundaries around backend services, maintaining strict network compartmentalization, and establishing the Computer Security Incident Response Team (CSIRT) structure spanning engineering, compliance, legal, and operational leadership.

Phase 2: Detection & Analysis

Continuous monitoring via automated SIEM systems analyzes event logs from production database clusters and transaction endpoints. By leveraging heuristic alerts, security analysts instantly identify anomalies—such as SQL-injection attempts, suspicious administrative query volumes, or credential-stuffing behaviors.

Phase 3: Containment, Eradication, & Recovery

Upon validating an active threat, containment protocols isolate compromised networks (e.g., disconnecting a compromised application server instance from the live transactional database environment). Eradication steps require identifying root vulnerabilities, neutralizing malicious payloads, and performing full forensic audits. Recovery safely returns services back to baseline production states while maintaining continuous operational monitoring.

Phase 4: Post-Incident Activity

No incident cycle is complete without a formal lessons-learned analysis. The CSIRT reviews metrics such as MTTD (Mean Time to Detect) and MTTR (Mean Time to Respond). Findings are translated directly into updated firewall rule sets, software patch validation routines, and continuous deployment pipeline improvements.

3. Business Continuity (BC) Model (ISO 22301)

While Incident Response focuses on containing active technical threats, Business Continuity Planning (BCP) preserves broader business functionality. Utilizing guidelines from the ISO 22301

standard, FinSecure designs its systems to maintain essential business workflows under adverse conditions.

The Business Impact Analysis (BIA)

The BIA identifies and prioritizes business critical systems using two core metrics: Recovery Time Objective (RTO)—the target duration of downtime before significant operational damage occurs; and Recovery Point Objective (RPO)—the maximum tolerable data loss window measured in back-up transaction times.

Business Function	Criticality	Target RTO	Target RPO	BCP Recovery Strategy
Transaction Processing	Critical	< 15 Minutes	Near-Zero (RPO ~ 0)	Multi-region active-active database clustering.
Online Portal Access	High	< 2 Hours	< 15 Minutes	Load-balanced web servers across cloud AZs.
Loan & Investment Portals	Medium	< 12 Hours	< 4 Hours	Scheduled offsite daily backups; secondary cold standby.

4. Technical Disaster Recovery (DR) Models & Crisis Management

To fulfill near-zero transaction loss objectives, FinSecure leverages physical and cloud-based architecture separation models:

Multi-Region Active-Active (Hot Standby): Critical transactional databases run concurrently in dual regional availability nodes. Real-time data synchronization ensures instant operational failover without transactional service degradation.

Warm Standby (Pilot Light): Secondary nodes (such as loan approval processing) run in a minimal scaled state. Upon main-site degradation, automation frameworks scale processing infrastructure up to full runtime capabilities.

Crisis Management Methods

When a technical outage threatens FinSecure's regulatory standing or customer relationships, the Crisis Management Team (CMT) is activated:

- **Command and Control (C2):** A clear escalation hierarchy is led by a designated Crisis Commander. This structures unified coordination, mitigating fragmented decision-making.
- **Regulatory Notification:** Legal and security compliance branches ensure rapid communication of critical data breaches to regulatory frameworks (such as the FCA or GDPR authorities) within designated operational timelines (e.g., 72 hours).
- **Public Relations & Customer Assurance:** Direct, clear channels issue transparent platform updates to users, reinforcing asset security and minimizing reputational risk.

Tactical Summary Playbook Scenario: In a SQL-injection containment event, the CSIRT isolates affected nodes (Incident Response), switches live database clusters to clean standby servers (Business Continuity), and updates regulatory bodies and public feeds simultaneously (Crisis Management), maintaining seamless alignment across all operational frameworks.