Crisis Response Framework (CRF)

Emergency Management & Incident Response Protocol

CONFIDENTIALITY NOTICE

This document contains critical crisis response procedures. Unauthorized access or distribution could compromise the Bank's ability to respond effectively to emergencies.

1. Objective

To ensure the Bank can respond swiftly and effectively to crises — financial, operational, cyber, or reputational — minimizing impact to customers, stakeholders, and regulatory standing.

2. Crisis Management Committee (CMC)

Role	Responsibility
CEO (Chair)	Declares crisis status, directs all major responses
CRO	Risk containment and recovery planning
Chief Information Security Officer (CISO)	Manages cybersecurity or system breach incidents
Head of Communications	Manages stakeholder, media, and regulatory communication
Chief Compliance Officer (CCO)	Ensures legal and regulatory adherence during crisis
Chief Operations Officer (COO)	Activates BCP and ensures service continuity

3. Crisis Classification

Level	Description	Example
Level 1 (Operational)	Localized incident, limited service impact	Regional outage
Level 2 (Critical)	Multi-site disruption, financial or regulatory implications	Data breach
Level 3 (Strategic)	Threat to solvency, customer trust, or license	Systemic fraud, insolvency

4. Response Protocol

- **Immediate Assessment: CMC convenes within 60 minutes of incident detection**
- **Containment: Isolate impacted systems, suspend compromised accounts, activate alternate data centers**
- **Communication: Public, regulator, and client updates within 24 hours**
- **Recovery: Restore full services via BCP**
- **Post-Mortem: Root-cause analysis, risk control enhancements, and Board-level review**

5. External Coordination

- Liaison with regulators (SEC, FinCEN, BOT, MAS)
- Communication with correspondent banks and partners
- Mandatory regulatory reporting for material incidents
- Legal counsel engagement for potential litigation or regulatory action

6. Crisis Communication Policy

All external statements are vetted by Legal & Communications to prevent misinformation. Media, regulators, and customers are informed only via verified channels. A 24/7 crisis hotline is activated for customer inquiries.

CMC Activation Triggers

CMC is automatically activated for: (1) System outages >4 hours, (2) Data breaches affecting >100 customers, (3) Regulatory enforcement actions, (4) Fraud losses >USD 50,000, (5) Major media coverage threatening reputation.