Business Continuity and Disaster Recovery

CORPORATE POLICY

Bank of America governs its Business Continuity and Disaster Recovery program through an established and documented corporate policy approved annually by the Board of Directors. Bank of America and its affiliates recognize the importance of protecting its employees, customers and clients through industry-leading management and practices of business continuity and disaster recovery. Those practices enable critical business functions and supporting technology, infrastructure and architecture to be defined, tested and maintained, and in the event of a business interruption, rapidly recovered.
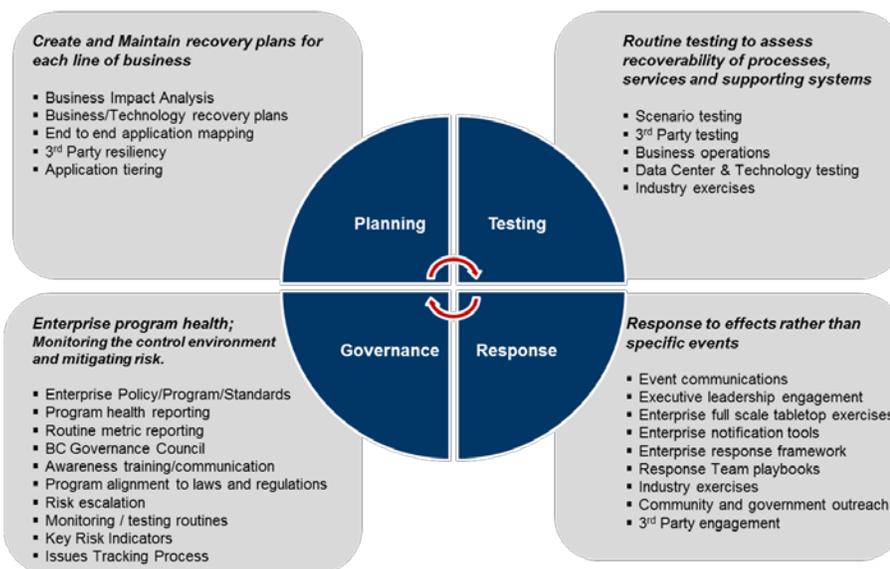
The Business Continuity and Disaster Recovery Policy applies to all employees of Bank of America and its third-party vendors and partners. It establishes minimum requirements for reasonably maintaining the availability of business functions after a business interruption. The policy includes defining, maintaining and testing recovery plans for critical business functions and technology applications within all of Bank of America's lines of business, internal support organizations and third-parties, so that they can remain operational after a business interruption.

PROGRAM OVERVIEW

The program focuses on assessing enterprise readiness for business interruption, accounting for employees and assembling leaders to execute their business continuity plans. The goal is to provide uninterrupted service to customers and clients by recovering critical business functions and applications.

The program is examined periodically by internal auditors and bank examiners and is designed to meet or exceed regulatory requirements and financial industry standards in all countries where Bank of America conducts business.

Business Continuity Lifecycle

Create and Maintain recovery plans for each line of business (Planning)
- Business Impact Analysis
- Business/Technology recovery plans
- End to end application mapping
- 3rd Party resiliency
- Application tiering

Routine testing to assess recoverability of processes, services and supporting systems (Testing)
- Scenario testing
- 3rd Party testing
- Business operations
- Data Center & Technology testing
- Industry exercises

Enterprise program health; Monitoring the control environment and mitigating risk. (Governance)
- Enterprise Policy/Program/Standards
- Program health reporting
- Routine metric reporting
- BC Governance Council
- Awareness training/communication
- Program alignment to laws and regulations
- Risk escalation
- Monitoring / testing routines
- Key Risk Indicators
- Issues Tracking Process

Response to effects rather than specific events (Response)
- Event communications
- Executive leadership engagement
- Enterprise full scale tabletop exercises
- Enterprise notification tools
- Enterprise response framework
- Response Team playbooks
- Industry exercises
- Community and government outreach
- 3rd Party engagement

GOVERNANCE

The program is managed centrally and provides oversight and direction for enterprise operational risks related to business continuity activities.

PLANNING

All divisions and subsidiaries must develop and maintain recovery plans commensurate with the criticality of the business function(s) as required under the established corporate policy. The criticality of a function is determined by a business impact analysis, which helps determine the recovery strategy, recovery time objective, recovery point objective and frequency of testing. Each recovery plan adheres to a standard development process and meets specific design requirements.

TESTING

Both functions and their supporting technologies within Bank of America are included in a comprehensive enterprise testing program that assesses and validates controls, recovery capabilities, and response readiness for the company and its third-parties to ensure they can operate as expected during a business interruption. (This is inclusive of industry bodies, Financial Market Utilities and payment systems to ensure continued services in the event of a business disruption)

The frequency of testing is determined by the criticality of the business function and its supporting technologies. Testing of the most critical functions is performed at least annually. Bank of America's business continuity and disaster recovery testing program is adhered to globally. Test results and compliance are monitored consistently by the business continuity organization.

RESPONSE

Across the enterprise, Bank of America has dedicated response teams with defined communications processes to ensure rapid dissemination of important information to customers, clients, employees, third-parties and government authorities affected by a business disruption.

The response process includes:

- Managing both readiness and response execution at times of crisis, and engaging critical external partners.
- Maintaining and expanding external Business Continuity & Disaster Recovery engagements in public and private sectors to enable world-class resiliency.
- Enhancing emerging-risk management across the enterprise and enabling readiness through a robust, annual exercise schedule.

RECOVERY RESOURCES

People

Employee safety is of the highest priority at Bank of America. All business continuity plans include procedures for addressing unavailability of staff during a business disruption, including a pandemic. Bank of America's pandemic planning is designed in accordance with country health agencies and government advice to ensure the protection of our employees and maintain critical functions over an extended time.

Facilities
As part of its commitment to providing uninterrupted service to customers and clients, Bank of America's business continuity plans include geographically dispersed backup facilities and other recovery locations for critical business processes, including off-site command centers, to direct recovery activities.

Technology
Mainframes
Around the globe, Bank of America has major data centers, including company-owned and vendor-managed facilities. An extensive array of advanced recovery technologies is employed to help ensure that recovery can be accomplished within agreed-upon time objectives. Critical customer data and application services are backed up electronically and to physical tapes, and intraday transactions are recorded to allow recovery to the point of a disaster. Tests of the recovery plans are conducted regularly for mainframe systems.

Midrange/Client Servers
Bank of America uses a variety of midrange/client server systems located throughout the enterprise. Recovery solutions are driven by the business functions supported by each system, and recovery plans are scaled to both the individual system and the entire data center in which hardware resides.

PROGRAM SUMMARY
Business continuity and disaster recovery planning at Bank of America is supported by an extensive program and incorporated into virtually every aspect of the company's business processes.

The business continuity program balances reasonable assessments of risk, placing the highest priority on the physical safety and security of our customers and employees, while preparing for loss of facilities and technologies. Our long history of resilience during disruptive events — from small occurrences, such as single building power outages, to large disasters, such as major hurricanes or tsunamis — demonstrates both our commitment to excellence and our ability to deliver on that commitment.

Bank of America cannot always guarantee a specific recovery time following a disruption caused by large-scale events that may include government breakdown or widespread interruption of public services. In those circumstances, Bank of America will make every reasonable effort to resume normal business as quickly as possible.

Last revised December 2018