Business Continuity and Operational Resiliency Program Overview

Methodologies

Business Continuity and Operational Resiliency (BCOR) are the methodologies used to prepare and respond to a business disruption, operational stress, and severe enterprise impact events. Serious incidents/threats, financial stress, and disasters, such as severe weather, technology outage, pandemics, geo-political events, and terrorism, are just a few examples of disruptions that could impact the welfare of our business and employees.

Governance

The BCOR Program at Bank of America is governed by an established corporate policy, which is reviewed and approved annually by the Board of Directors. Bank of America and its affiliates recognize the importance of protecting employees, customers, and clients through an industry-leading management of business continuity and operational resilience.

Those practices enable critical business functions, services, technology, data, infrastructure, and third parties to define, rate criticality, test, maintain, mitigate, restore, and recover in the likelihood of a business disruption event, including severe operational stress events.

Maintaining the availability of business functions and services

The BCOR program incorporates both business continuity and operational resiliency approaches to maintaining the availability of business functions and services.
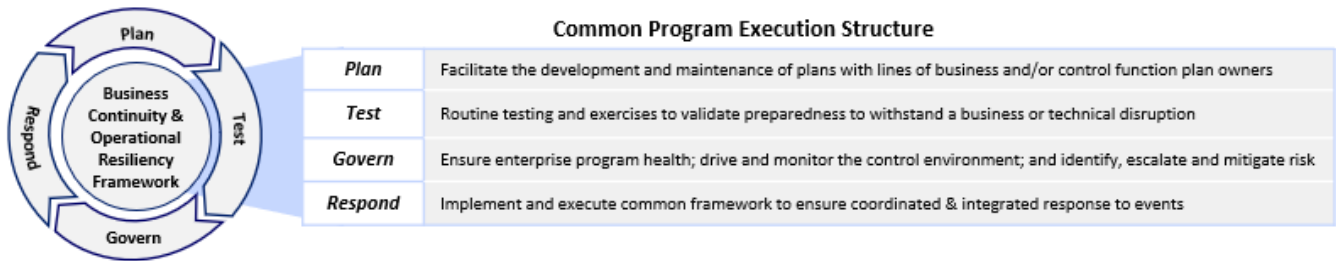
Business Continuity provides the methodology for preparing for and responding to a business disruption event enabling critical business functions, technology, infrastructure and supporting third parties to continue with minimal interruption or impact.

Operational Resiliency is an elevated level of preparedness and capabilities (from business continuity) that incorporates proactive, business-driven strategies for mitigating the risk and impact of a severe business disruption event in the overall design of operations and processes. It focuses on the company's ability to anticipate, prevent, minimize, respond to, mitigate, recover from, and learn from operational stress and severe enterprise impact events.

The BCOR Program drives consistency across regions while incorporating unique jurisdictional requirements to ensure adherence to applicable laws and regulations.

Program execution

Robust execution of the Business Continuity and Operational Resiliency Program using a common program execution structure of Plan, Test, Govern and Respond enables Bank of America to establish and demonstrate preparedness to respond to and recover from events across the continuum and to establish capabilities to drive and enhance the bank's resiliency.

Common Program Execution Structure

Plan	Facilitate the development and maintenance of plans with lines of business and/or control function plan owners
Test	Routine testing and exercises to validate preparedness to withstand a business or technical disruption
Govern	Ensure enterprise program health; drive and monitor the control environment; and identify, escalate and mitigate risk
Respond	Implement and execute common framework to ensure coordinated & integrated response to events

PLAN - Planning is a core component of the BCOR Program as it establishes minimum requirements for a front-line unit or control function (FLU/CF) to maintain the availability of business functions, services, and applications in the event of a business interruption.

TEST - Resilience Testing and Exercise provides a multi-faceted and comprehensive structured approach to validating Bank of America's preparedness to withstand a business or technical disruption.

GOVERN - Governance establishes structure, manages policy standards, oversees compliance with regulatory requirements and enterprise policies, and outlines measurement, reporting and escalation, and quality assurance of program results.

RESPOND - In close coordination with front line units and control functions, the Global Response organization maintains end-to-end accountability for implementing and executing a common framework to ensure a coordinated and integrated response to events that might directly or indirectly impact Bank of America.

Resources

PEOPLE - In keeping with Bank of America's focus on resiliency in the face of a business disruption, all business continuity plans include procedures for addressing temporary unavailability of staff during natural disasters, pandemics, unplanned outages, and other events.

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 and resilience activities.

TECHNOLOGY – Bank of America establishes requirements for resiliency and enhanced technology capabilities that support execution of planning, testing and governance. With a Global footprint, Bank of America both leverages its vast network of Data Centers and Facilities for resiliency capabilities, as well as monitors and validates the function of each location for resiliency purposes. This is done through a combination of Resiliency monitoring including Enterprise Critical Infrastructure, Application Technology and Data Management.

ENTERPRISE CRITICAL INFRASTRUCTURE – Bank of America has established guidelines for the continuity and resiliency of critical infrastructure.

APPLICATION TECHNOLOGY – Bank of America has a comprehensive, enterprise-wide technology resiliency planning and testing program, to ensure application preparedness for a Location outage or cybersecurity attack. Application recovery plans and application restoral plans are assessed during scheduled, location-based testing to demonstrate recovery and/or restoral within target business objectives. Plans and tests are subject to compliance requirements, including quality assurance reviews and regular technology management approvals, and compliance metrics are reported to senior leadership.

DATA – Bank of America has developed data capabilities designed to provide a consistent, repeatable approach to prepare for, prevent, and recover from data corruption and other data impacting events.

THIRD PARTY – Third parties providing critical service and technology solutions are included in a comprehensive enterprise testing and assessments program that validates controls, recovery and resilience capabilities, and response readiness to ensure that, during a business disrupting event, the third party is operational. The bank's third-party testing and assessments program is adhered to globally.

Close

Bank of America's long history of resilience during disruptive events — from small occurrences, such as single building power outages, to large disasters, such as pandemics, major hurricanes, or tsunamis, and to long-term third-party disruption — demonstrates our commitment to excellence and our ability to deliver on that commitment.