

BUSINESS CONTINUITY MANAGEMENT

Corporate & Investment Banking Americas

August 2016

From the Corporate & Investment Banking Americas Executive Committee

Business Continuity Management (BCM) is an essential part of how Natixis Corporate & Investment Banking (CIB) Americas conducts its business. To ensure continued business operations and service delivery to our clients and counterparties, while protecting our staff and assets, in the event of a business interruption, we are committed to an active and robust Business Continuity Program. The BCM Team is responsible for the development of enterprise level business recovery strategies. It works closely with our business and support lines to provide recovery capabilities at an alternate location as well as Business Continuity Plans and all related testing and awareness activities.

Business Continuity Drivers

Natixis CIB Americas is committed to a BCM program that:

1. is consistent with sound enterprise risk management practices and business resiliency models
2. promotes employee safety and crisis management awareness
3. protects the firm's assets, both physical and virtual (data), and brand name
4. allows the firm to honor external obligations and participate in critical business activities
5. satisfies all regulatory and legal requirements
6. maintains the firm's competitive advantage and client expectations in the marketplace

Organization

The BCM team is proactively and heavily engaged not only with all internal Natixis CIB Americas business areas and functions but also with external industry related groups and practices. The function reports to the Executive Security Committee with a reporting line into the Chief Risk Officer. The mission and objectives of the BCM team are to:

1. develop and implement business continuity programs, policies, and standards firmwide
2. develop, implement, and maintain a crisis management program, including incident response activities
3. provide business impact and risk assessment analysis on the firm's recovery strategy solution
4. develop, implement, and maintain plan documentation for usage of all business recovery activities including supporting BCM tools
5. provide testing and training awareness activities to the firm to validate all BCM components

At Natixis CIB Americas, BCM operates under the sponsorship and oversight of the Executive Security Committee (ESC) comprised of senior executives. The ESC makes all decisions about the program resources and recovery capabilities the firm will implement. The CIB Americas BCM program is closely aligned and consistent with business continuity organizations from our head office in France regarding policies, global standards and reporting.

Internally BCM relies upon a network of sponsors, liaisons, and coordinators within each business unit so the planning process includes the business knowledge required to develop a comprehensive recovery plan. Single points of contact within each business unit ensure that all BCM initiatives are introduced and implemented at the business unit level.

The BCM team also works closely with our internal partners to define, develop, and implement BCM program components that make our business more resilient and recoverable in the event of a business interruption. Our primary internal partners include Information Technology/Disaster Recovery (IT/DR), Facilities, Communications, Human Resources, Compliance, Operational Risk, and Audit.

Program Components

Natixis' CIB Americas BCM team's program, comprised of several components that are recognized best practices, is subject to regular and cyclic maintenance activities. These components are:

- 1. Recovery Strategy Development and Implementation.** The development and implementation of the recovery strategy is a result of a significant amount of analysis concerning businesses impacts, risk, recovery requirements, and costs consolidated from each business unit to the enterprise level. With our partners in the IT/DR area, BCM utilizes these data to produce robust recovery strategies that consider both the technology and personnel aspects.
- 2. Crisis Management Program.** Anchored by the Crisis Management Team (CMT) comprised of all senior executive and relevant functional heads, this program is the Command and Control of all firmwide crisis and recovery decisions. The program also includes logistics information, communications plans, command centers, focused planning considerations, i.e., pandemic, and firmwide internal and external contact information.
- 3. Plan Products.** BCM helps the firm and each business line develop and maintain various types of BCM plan products, including business continuity plans, call trees, staff emergency instruction wallet cards, a crisis management framework (plan), crisis management wallet cards, and an incident escalation framework and emergency instructions leaflets.
- 4. BCM Tools.** BCM regularly uses a wide array of supporting tools during program development and actual incident response, including an Emergency Notification System, BCM Database and Planning tool, BCM intranet site, Emergency Hotlines, Command Centers, and Corporate Emergency Access System (BNet).
- 5. Testing Program.** BCM has a robust testing program that proves our capabilities and identifies areas for remediation. The types of tests performed are:
 - disaster recovery data center testing
 - recovery seat testing
 - remote access testing
 - crisis management tabletop testing
 - industry-related testing (e.g. SIFMA)
 - emergency notification system testing
- 6. Training and Awareness.** BCM conducts a training and awareness program that enrolls our sponsors, owners, partners and coordinators and provides a New Hire training to all employees that focus on BCM. In addition, all employees are required to participate in a Business Continuity Awareness Training session each year to ensure continued awareness of the Firm's Business Continuity Management program and our employees' roles during a business interruption.

Recovery Strategy and Capability

BCM has developed a recovery strategy that covers all business lines and relies upon the use of pre-positioned firmwide recovery assets. This strategy covers multiple scenarios by operating on a dual matrix of scenario definition including local vs. regional events and denial of access vs. full DR events.

The majority of the mission-critical functions for Natixis CIB Americas reside in Manhattan. Natixis has independent production and backup data centers and a business recovery space. Between this dedicated space and remote access capabilities, Natixis CIB Americas can host a significant proportion of its total employee population for a significant length of time.