Morgan Stanley

Business Continuity Management Program and Technology Disaster Recovery Program Overview

Purpose and Governance

Morgan Stanley maintains global programs for business continuity management and technology disaster recovery that facilitate activities designed to protect the Firm during a business continuity event. A business continuity event is an interruption with potential impact to normal business activity of the Firm's people, operations, technology, suppliers, and/or facilities.

The business continuity program's core functions are business continuity planning (with associated testing) and crisis management. The Firm has dedicated Business Continuity Management staff responsible for coordination of the program governed by the Business Continuity Governance Committee and a Risk Oversight Committee. In addition, a Committee of the Board of Directors (the "Board Committee") and senior management oversee the program. BCM reports to the Board Committee at least annually on the status of program components such as business continuity events and business continuity testing results.

Business Continuity Planning

Business Units within the Firm maintain business continuity plans, identifying processes and strategies to continue business critical processes during a business continuity event. Business Units also test the documented preparation, to provide a reasonable expectation that, during a business continuity event, the Business Unit will be able to recover and perform its critical business processes and limit the impact of the event to the Firm and its clients.

As part of business continuity planning, Business Units must identify and assess the potential impact of threats that may significantly disrupt their business or the business operations of the Firm. Business Units conduct a Business Impact Analysis to prioritize their business processes, which is then reviewed and signed-off, typically on a semiannual basis.

Business continuity plans document recovery strategies (e.g., transference or relocation) that identify and detail the options available to recover critical business processes during an event. The plans also identify roles and responsibilities and communication procedures when plans are invoked for an event. Business continuity plans are reviewed by business unit management, typically on a semiannual basis, and disseminated to staff at least annually.

Business Units are responsible for periodic testing and documentation of test results in accordance with Firm testing requirements. Business continuity testing is the process by which Business Units verify the viability of their plans by performing their critical business processes using the recovery strategies documented in the plans.

Business Continuity Crisis Management

Crisis Management is the process of identifying and managing the Firm's operations during business continuity events. BCM monitors and assesses situations for the impact on business operations and to determine their potential to become business continuity events.

BCM staff are responsible for escalating business continuity events to Firm management and designated personnel, as appropriate. BCM coordinates and facilitates the exchange of information between those charged with resolving the situation, senior management, and the Business Units that are impacted.

The Firm's crisis management process also includes coordination of internal and external communication to key stakeholders, including personnel, regulators, suppliers, and customers. BCM oversees a mass notification system that can be utilized during an event, and ensures that the system is regularly tested.

Business Continuity Training and Awareness

The Firm has developed a program for providing business continuity training, at least annually, to all personnel. Training is designed to promote an understanding of business continuity, as well as the roles of BCM and personnel during a business continuity event and as the business recovers. Personnel are responsible for completing the training and familiarizing themselves with their Business Unit Coordinators and business continuity plans.

Business Continuity Supplier Risk

The Firm assesses and performs risk-based due diligence on third-party service providers' resiliency and ability to continue to provide services during an event. As part of that assessment and due diligence, BCM, in conjunction with the Technology Disaster Recovery group and the appropriate Business Unit, evaluates vendors and suppliers of in-scope services, in support of the Firmwide Third Party Program Management group. Assessments of in-scope critical vendors are repeated periodically, but no less than annually. Technology testing with these vendors is conducted periodically, as appropriate.

For specific vendor locations where vendor staff provide services on behalf of the Firm using Firm data and support a critical business process, the Business Unit and/or the central management group for these vendors must develop and maintain a business continuity plan for the vendor. The plan for the vendor must meet Firm standards for business continuity planning.

Business Continuity Pandemic Preparedness

BCM, in conjunction with the Firm's Human Resources and Corporate Services Departments, maintains an Infectious Disease Preparedness Procedure to address planning for potential pandemics. The Procedure documents precautionary measures that the Firm can take to help reduce business impact should the Firm's operations be affected by an infectious disease outbreak, epidemic, or pandemic event. BCM can invoke these procedures based on pandemic warnings from the World Health Organization, the Centers for Disease Control and Prevention, and/or other official local governance bodies.

Technology Disaster Recovery

Morgan Stanley's primary data centers are built to be redundant, resilient and fault tolerant. Disaster recovery plans supporting business continuity are in place for critical technology assets across the Firm.

Recovery capabilities are tested regularly to confirm that technology assets will operate as intended during a business continuity event.