Morgan Stanley

Business Continuity Management Program

Notice: The information contained herein is for informational purposes only, and no warranty of any kind is intended with respect to the systems or business practices described. Provision of this information does not entitle the recipient to any contractual right that the practices described in the attached materials will continue to be maintained.

Purpose and Governance

Morgan Stanley's Firm Resilience organization maintains global programs for Business Continuity Management (BCM), Disaster Recovery (DR) and Third Party Resilience that facilitate activities designed to protect the Firm during a business continuity incident. A business continuity incident is an interruption with potential impact to normal business activity of the Firm's personnel, operations, technology, suppliers, and/or facilities.

The Firm Resilience organization has dedicated staff responsible for management of the aforementioned programs which are governed by the Business Resilience Governance Committee. In addition, a Committee of the Board of Directors and senior management oversee the program.

Business Continuity Planning

The Global Business Continuity Planning Procedure sets forth the standard set of processes and operating instructions for Business Units within the Firm to develop business continuity plans and identify processes and recovery strategies to continue business critical processes during a business continuity incident.

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 at least annually.

Business continuity plans document recovery strategies (e.g., transference or work area recovery) that identify and detail the options available to recover critical business processes during an incident. The plans also identify roles and responsibilities and communication procedures when plans are invoked for an incident. Business continuity plans are reviewed and signed off by Business Unit management at least annually.

Business Units are responsible for periodic testing and documentation of test results in accordance with the requirements set out in the Global Business Continuity Testing Procedure. 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 testing and documentation of test results provide a reasonable expectation that, during a business continuity incident, the Business Unit will be able to recover and perform its critical business processes and limit the impact of the incident to the Firm, its clients, and financial markets.

Crisis Management

The Crisis Management Team which forms part of the Fusion Response organization is responsible for Crisis Management, the process of identifying and managing the Firm's operations during a business continuity incident. In conjunction with the Global Threat Intelligence team, Crisis Management Operations monitors and assesses situations for the impact on business operations and to determine their potential to become business continuity incidents.

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

The crisis management process includes coordination of internal and external communication to key stakeholders, including personnel, regulators, suppliers, and customers. Crisis Management Operations oversees a mass notification system that can be utilized during an event to contact staff and ensures that the system is regularly tested.

Business Continuity Pandemic Preparedness

BCM, in conjunction with the Firm’s Chief Medical Officer, Human Resources, and Corporate Services Departments, maintains a Global Business Continuity 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 business continuity incident. The Firm 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.

Business Continuity Training and Awareness

Business Continuity Management is responsible for developing, providing, and tracking completion of Business Continuity Role Holder attestation training. This training is designed to ensure that those personnel involved in the Business Continuity Management process and involved in recovery during a business continuity incident are aware of their roles and responsibilities.

Business Continuity Third Party Risk Management

The Firm assesses and performs risk-based due diligence on third-party vendors business continuity and disaster recovery controls and ability to continue to provide services during a business continuity incident.

Third Party Resilience performs exercises with third party vendors and develop contingency and exit plans in partnership with the business units in order to manage service disruption risk and build firm resilience. Business Continuity Tabletop Exercises validate recovery of non-technology elements (people and buildings) for non-technical services. These tests are repeated periodically during the life of the service, following a risk-based approach.

For specific vendor locations where vendor staff provide services on behalf of the Firm using 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 in alignment with Firm standards.

Disaster Recovery

The Technology Planning, Testing & Readiness program oversees the documentation of Technical Recovery Plans and disaster recovery testing of critical Firm systems and third parties in order to validate recovery capability. Technical recovery plans are in place for critical technology assets and document how systems would be recovered following a disruption.