Morgan Stanley

Firm Resilience and Crisis Management Program Overview

Purpose and Governance

Morgan Stanley's resilience program is supported by dedicated teams within Firm Resilience and Fusion Response. The Firm Resilience organization maintains global programs for Business Continuity Management (BCM), Disaster Recovery (DR), Third Party Resilience and Key Business Service Resilience (collectively, the "Firm Resilience programs"), which are designed to protect the Firm while remediating a business continuity incident. During a business continuity incident, the Fusion Response organization leads a rapid and comprehensive response and recovery operation in order to minimize business disruption. A business continuity incident is an interruption with potential impact to normal business activity of the Firm's personnel, technology, suppliers, and/or facilities. Such incidents might result from cyber-attacks, failure or loss of access to technology and/or associated data, military conflicts, acts of terror, natural disasters, severe weather events and infectious disease, as examples.

The programs identify criticality of processes and supporting assets, identify options to recover assets during an incident, and establish the command and control structure for incident management. The programs are tested annually.

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

Key Business Service Resilience

The Firm's Key Business Services (KBS) Resilience program has in place an operational resilience assessment framework used to integrate resilience considerations into existing risk management and governance models.

Through this program, Firm Resilience actively engages Business Unit stakeholders to identify KBS based on market, client and Firm impact, map dependencies and assets for KBS, develop stress scenarios impacting the KBS and test such scenarios end-to-end to identify lessons learned so as to continuously enhance the program.

Business Continuity Planning and Testing

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) 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 Plan Testing Procedure. Issues identified through testing are addressed and tracked up to closure, and enhancements to business continuity plans are implemented as appropriate.

Business Continuity Pandemic Preparedness

The Firm maintains a Global Business Continuity Infectious Disease Preparedness Procedure to address planning for potential pandemics ("the Procedure"). 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 proactively monitors developments relating to potential pandemics to ensure the health and safety of our employees and their families, including pandemic warnings from the World Health Organization, the Centers for Disease Control and Prevention, and/or other official local governance bodies, and can invoke the Procedure as necessary.

Business Continuity Training and Awareness

Firm Resilience 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 are aware of their roles and responsibilities. Training is also provided to Business Continuity plan role holders on the use of Firm approved business continuity tool for performing business impact analysis and documenting of business continuity plans as appropriate.

Third Party Risk Management

The Firm assesses and performs risk-based due diligence on third-party service providers' business continuity and disaster recovery controls and their ability to continue to provide services during a business continuity incident through the third-party Business Continuity Assessment Program. The program assesses the service providers' alignment to the Firm's policies and standards through qualitative and quantitative analysis.

Firm Resilience supports the Business Units in developing Contingency and Exit plans in order to mitigate risk of business disruption due to service provider failure. Contingency and Exit Plans provide a documented operational response and recovery strategy to maintain or resume business or a critical business process in the event of a service disruption or a need to transition away from a service provider. These could include but are not limited to a service outage or loss of a service provider. Contingency and Exit Plans are required to be refreshed by Business Units on an annual basis.

For specific service provider locations where service provider 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 service providers must develop and maintain a business continuity plan for the service provider in alignment with Firm standards.

Business Continuity Exercises

The Firm's Exercise Program designs, sequences and delivers risk-based cyber, technology and business continuity exercises to enhance operational resilience and preparedness throughout the Firm and with our third parties. These are interactive, scenario-based exercises that simulate a full range of threat scenarios, including technology incidents, cyber-attacks and business disrupting events impacting people, property, and infrastructure. Through these exercises, the Firm tests and improves its preparedness to manage a variety of threats and risks.

Disaster Recovery Planning and Testing

The Disaster Recovery program oversees the documentation of Technical Recovery Plans and execution of Disaster Recovery testing of Firm systems and third parties in order to validate recovery capability. Technical Recovery Plans (TRPs) are in place for critical technology assets and document how systems would be recovered following a disruption. TRPs are required to include processes to failover a system between data centers, recover data in the event of a loss or corruption scenario and the 'ready for business' checks that would be performed to validate the system is available and functional following recovery. TRPs are periodically reviewed according to the criticality of the system at issue.

Disaster recovery testing is performed according to each asset's criticality (e.g. Tier-1 are tested annually) to confirm that technology assets will operate as intended during a business continuity incident. The scenarios in scope for disaster recovery include loss of application, loss of data center and loss/corruption of data.

Crisis Management

The Fusion Response organization is responsible for Crisis Management, the process of identifying and managing the Firm's operations during a business continuity incident. Fusion Response monitors and assesses situations for the impact on business operations, determines their potential to become business continuity incidents, and determines any necessary response to such incidents.

Fusion Response is responsible for escalating business continuity incidents to Firm management and designated internal personnel, as appropriate. Fusion Response also coordinates and facilitates the exchange of information between those charged with resolving the situation, senior management, the Business Units that are impacted and other relevant stakeholders as necessary.