Morgan Stanley

Firm Resilience and Crisis Management Program Overview

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 resilience program is supported by dedicated teams within Firm Resilience and Fusion Response organizations. 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. 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. During a business continuity incident, the Fusion Response organization will lead a rapid and comprehensive response and recovery operation in order to minimize impact from this broad range of business disrupting threats and incidents, and collaborate with partner organizations to understand, prepare for, and learn from these events.

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 and/or financial stability impact, map assets that support KBS, develop stress scenarios impacting the KBS and test such scenarios end-to-end to identify lessons learned to continuously enhance the resilience of KBS.

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 (BC) 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 the dependent assets (e.g. systems, teams) and associated recovery strategies (e.g., transference or work area recovery) to recover business critical processes following a BC incident. The plans also identify roles and responsibilities and emergency contact information when plans are invoked for an incident. Business continuity plans are reviewed and signed off by Business Unit management at least annually.

Business Continuity Plan testing continues throughout the year and covers the testing of dedicated, displacement, remote and transference recovery strategies across various loss scenarios. Test results are reviewed to ensure that any issues identified through testing are addressed and tracked up to closure, and enhancements to business continuity plans are implemented as appropriate. In addition, retest is scheduled where required, to ensure the issues have been resolved.

Business Continuity Pandemic Preparedness

The Firm maintains a Global Business Continuity Infectious Disease and Pandemic 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 & KBS 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 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.

To embed Operational Resilience across the Firm it is necessary to outline a clear, consistent, and comprehensive global view of what Operational Resilience entails, by ensuring each Morgan Stanley staff member understands their roles and responsibilities. This facilitates Morgan Stanley staff to successfully deliver Operational Resilience as an outcome. The training provides a common foundational understanding suitable for all staff, and also content bespoke to various capability areas and roles as relevant.

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 requires the Business Units to develop Contingency Plans and Exit Plans in order to mitigate risk of business disruption due to an outage or termination of critical third party services. Contingency Plans document the Firm’s planned operational response and recovery strategy to maintain or resume critical business processes in the event of a critical third party service outage, and Exit Plans similarly address the Firm’s operational response when it is necessary to permanently transition away from usage of a critical service. Contingency and Exit Plans are required to be refreshed by Business Units on an annual basis.

External Third Party locations which connect to Morgan Stanley infrastructure with External Third Party staff performing services on behalf of the Firm, are required to comply with the Global Business Continuity Management Policy and maintain business continuity plans in the Firm approved application as documented in the Morgan Stanley Offsite Delivery Center (ODC) Vendor Requirements Manual. Business Units, whose business functions are outsourced, are responsible for reviewing and approving such plans and crisis management documentation and ensuring interoperability with their own BC Plans.

Resilience Testing & Exercises

The Firm designs, sequences and delivers risk-based cyber, technology and business continuity exercises and technical recovery tests to enhance operational resilience and preparedness throughout the Firm and with our third parties. These are scenario-based tests and exercises that simulate a full range of threats, including technology incidents, cyber-attacks and business disrupting events impacting people, property, and infrastructure. Through these tests and exercises, the Firm validates and improves its preparedness to manage a variety of threats and risks. For further details on business continuity and disaster recovery testing, refer to the section “Business Continuity Planning and Testing” and “Disaster Recovery Planning and Testing” respectively.

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 external services 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.

Disaster recovery capability is tested at a frequency in line with the technology asset’s criticality (e.g. Tier-1 are tested annually) to confirm that technology assets will operate as intended during a business continuity event requiring failover to an alternate location.

In addition, the Firm’s Database Recovery Testing Program validates recovery capabilities for in-scope assets by restoring production back-ups to verify the accuracy and measure timeliness of the database restore capabilities.

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 detects, monitors and prepares for specific physical threats to Firm personnel, operations, and assets and leads response and recovery efforts as these threats materialize.

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.