April 2017

# Business Continuity Disclosure

## Revision History

| REVISION | DATE | NAME | DESCRIPTION |
|---|---|---|---|
| 1.0 | 4/26/2017 | Mandar Soman | Final |

## Review and Approvals

| REVISION | DATE | NAME | DESCRIPTION |
|---|---|---|---|
| 1.0 | 4/26/2017 | Joseph Monks | Final |

## Distribution

| REVISION | DATE | NAME | DESCRIPTION |
|---|---|---|---|
| 1.0 | 4/26/2017 | GMT | Final |

### *Purpose*

This document outlines the Business Continuity Plans (BCP) and procedures developed by MarketAxess Corporation (MAC). These plans guide the firm in promptly responding to business interruptions resulting in the loss of access to people, facilities, technology, or critical third party vendors and in restoring the services provided to MAC's clients within a reasonable timeframe.

### *Business Continuity Framework*

MAC has adopted a business continuity framework that focuses on reviewing all core components of the business to understand potential impact of a business interruption. This was developed through:

- Interviews with critical business functions to understand and prioritize the planned response.
- Review of existing policies and procedural documentation.
- Undertaking a Business Impact Analysis.

The end result of the Business Continuity Framework is a series of departmental playbooks that outline how MAC will respond to events that result in the loss or impairment of physical work locations, critical internal resources, supporting technology, or critical third parties. Refer Appendix-I for Maturity State of Business Continuity Program.

### *Response Approach*

In the event of a major business interruption, MAC will initiate its business continuity procedures which include, but not limited to;

- Initiate the crisis management plan and open relevant communication channels. The business impact analyses are also referenced to assess the potential impact of the business interruption.
- Evaluate incident to assess the client/3rd party impact and provide relevant and appropriate communication to clients and other relevant 3rd parties.
- Implement the response plans detailed in the BCP playbooks which provide detailed steps on how to act under the given situation.
- Implement the necessary and appropriate contingency plans for the recovery and resumption of services following the loss or impairment of people, process, technology or critical vendors.
- Evaluate any regulatory impact.

Based on the impact assessment and severity of the interruption, the following may also be required;

- Data recovery procedures to be invoked.
- Recovery of mission critical systems & processes (e.g. regulatory reporting) to be restored.
- Financial and operational assessments to be undertaken.
- Relocation of staff to an alternate physical location.
- Assess and invoke critical suppliers & vendors contingency plans.

### *Crisis Management Team*

A Crisis Management Team (CMT) has been established and is responsible for managing the organization's response to the business interruption and for communications related to the interruption. There are three teams that make up the overall Crisis Management Team:

- **Executive (Global & London) Management Team** is comprised of Senior Executive Leaders and is responsible for enterprise-wide strategic decisions.
- **Local Management Team** is comprised of Senior Management leaders of impacted business units / locations. This group is responsible for declaring crisis and communication with clients and other 3rd parties.
- **Business Recovery Team** is made up of key business function representatives. This team focuses on managing the tactical recovery activities.

#### ***Business Impact Analysis***

Each department (e.g. Finance, Production Support, IT Infrastructure, Client Services) conducted a Business Impact Analysis (BIA).

This process was a study of individual business processes and support functions in order to estimate the impact of downtime events, identify interdependencies between business process and support functions, identify critical technology, records, equipment and other infrastructure required and the recovery time objectives and recovery point objectives.

The results of each departments BIA was considered when determining system recovery priorities and the development of the departmental playbooks / plans.

#### ***Detailed Playbook/Plans***

An actionable BCP "Playbook" was then developed for each department outlining how that team will operate during a business interruption impacting the availability of physical location, resources, technology or vendors.

These plans are hosted by a third-party service provider to ensure that information is accessible in the event of networking / system access issues within MAC.

### *Communication*

Business interruptions are communicated to MAC personnel and clients as needed based on the nature, severity and urgency of the interruption. MAC has established several mechanisms to alert employees of a business interruption and provide additional instructions and information related to the event. These include:

- Business continuity hotline phone number.
- Two-way text paging mechanism.

All employees have been provided with additional information on each communication method.

### *Governance*

BCP governance is managed by the MAC Head of Infrastructure. Annual review and testing of the BCP is undertaken by the internal audit and risk function of MAC as part of its enterprise risk management function under the supervision of the MAC Head of Infrastructure.

#### *Periodic Testing*

Annually, MAC performs a disaster recovery test and an office availability test. The disaster recovery test is centered around data center unavailability and core server side systems whereas the office availability test focuses on the office being unavailable.

The tests ensure that the systems are accessible and fully functional end-to-end from secondary sites.

In addition to these tests, MAC also performs a BCP table top test exercise with all departments to assist management in evaluating the effectiveness of the BCP plans and the firm's readiness to implement the plans during a business disruption using realistic scenarios.

### *Recovery Times*

MAC operates a highly available service that has full redundancy and resilience built within its primary data center. It can withstand the loss of multiple components with minimal interruption. Data is protected to prevent data loss within the data center.

### *Recovery Point Objective (RPO)*

"RPO" represents the amount of data (in hours/days) that can be lost before there is unacceptable impact to the end-users. The recovery point objective (RPO) stands at 1 minute.

### *Recovery Time Objective (RTO)*

"RTO" represents the span of time between the occurrence of the business interruption through to the time that applications and data are available in some capacity to business users and external stakeholders. The maximum target recovery time of all critical client facing systems MAC applications is 6hrs (RTO), with previous testing demonstrating recoverability within 3hrs.

### *Overview of Business Continuity Contingency Plans*

### *Data Center*

In the event of a failure, MAC would fail over to one of the backup data center locations. The service level is to be up and running within six hours after declaration of disaster and decision is made to enable our disaster recovery site. MAC Data Centers are located at:

- US: New Jersey - Primary Production Data Centre.
- US: Virginia - Backup Data Centre.

The data centers are located over 200 miles apart to minimize simultaneous risk to power or physical disasters.

### *Offsite Locations*

In the event of a loss of physical facilities in New York, MAC systems, processes and staff would operate through enacting its BCP procedures. These include remote working and use of the BCP site as follows;

- A designated approver contacts SunGard to initiate the contingency plan.
- MAC Infrastructure Team will report to SunGard and prepare the agreed upon equipment.
- Designated staff will report to the SunGard facility located at assigned alternate site in New Jersey, US.

### *Non-Critical Staff*

This section summarizes the contingency procedures should an outage occur at a main facility. Since certain areas have been deemed non-critical to the operation of the organization, the following assumptions are made:

- PC's will be readily available from local vendors for those employees who do not have a PC to work from home.
- Analog telephone service is available at home for every employee.
- All Sales employees and critical development staff have laptops and the ability to send and receive email remotely via smartphones.
- A lead-time of 7 days to set up individuals is acceptable since these are not considered business critical functions.

### *Additional Considerations*

- MAC has capabilities to utilize corporate resources and facilities in New York and London.
- These include;
    - Offsite BCP facilities in New Jersey, US and London provided for by SunGard.
    - Data Center Facilities in two physically separated sites in New Jersey and Virginia, which have redundant capabilities for all critical systems.
- Telephone services that can operate independently in each location.
- Risk of pandemic disease is reduced due to corporate staff in multiple countries, all of whom are capable of operating our systems.
- This BCP does not address how MAC would assure customers' prompt access to their funds and securities in the event MAC would determine that it would be unable to continue its business as MAC does not hold customer funds or securities.

***Disclaimer***

This disclosure summarizing the MAC Business Continuity Plan (the "BCP") is accurate as of 8th of April 2017 and both this disclosure and the BCP are subject to change at the discretion of MAC at any time and for any reason. MAC makes no representations that this disclosure or the BCP will remain intact for any period of time.

MAC disclaims any and all warranties, express or implied, related to the MAC Business Continuity Plan and this disclosure. This disclosure is written for external review; therefore certain confidential and proprietary details have been intentionally omitted.

# Appendix-I

## MAC Business Continuity Program – Maturity State as of April 2017