BUSINESS CONTINUITY DISCLOSURE 2025

Disclaimer
This disclosure is only intended for subscribers to the Company's services as a summary of the Company's Business Continuity Management (**BCM**) and while it is accurate as of January 2025, both this disclosure and the Company's BCM are subject to change at the sole discretion of the Company (or any of its subsidiaries) at any time and for any reason. In the event of any discrepancy between this disclosure and the Company, the Company makes no representations that this disclosure or the BCM will remain intact for any period of time. Neither the Company nor any of its group companies accept any obligation to provide you with access to any additional information or to update this disclosure.

This disclosure is provided without any warranty (express or implied), condition, guarantee or representation of any kind by the Company and its affiliates (and any of their respective directors, officers, agents, contractors, interns, suppliers and employees) and shall not be responsible, nor have any liability for any damage, loss, expense, claim or cost of any nature howsoever arising from, or in connection with, any use of the disclosure. This disclosure is not legally binding, and it does not govern any aspect of the Company's services, delivery of which is solely provided for in the relevant Service Order Form and Master Agreement.

This disclosure is written for external review, therefore certain confidential and proprietary details have been intentionally omitted.

This disclosure applies to MarketAxess Holdings Inc. and each of its subsidiaries.

TABLE OF CONTENT

1 PURPOSE 4
1.1 SCOPE 4
1.2 DOCUMENT MAINTENANCE DISCLOSURE 4
2 BUSINESS CONTINUITY MANAGEMENT 4
2.1 APPROACH 4
2.2 BCM FRAMEWORK 5
2.3 CRISIS MANAGEMENT STRATEGY 6
2.4 RECOVERY TEAM STRUCTURE 7
3 BUSINESS CONTINUITY PLAN 7
3.1 CRISIS MANAGEMENT PLAYBOOK 7
3.2 BUSINESS IMPACT ANALYSIS 8
3.3 DETAILED PLAYBOOK/PLANS 8
3.4 OFFSITE LOCATIONS 8
3.5 THIRD-PARTY SERVICE PROVIDERS 9
4 DISASTER RECOVERY 9
4.1 DATA CENTERS 9
4.1.1 Recovery Times 9
4.2 SYSTEMS AND SERVERS 9
4.3 BACKUP OVERVIEW 10
4.4 CRISIS MANAGEMENT SCENARIOS 10
5 PANDEMIC (E.G.: COVID-19) 11
6 TESTING, AWARENESS AND DOCUMENTATION 12
6.1 2024 RESULTS 13
7 COMMUNICATION 14
7.1 EMPLOYEE COMMUNICATIONS 14
7.2 CLIENT COMMUNICATIONS 14
7.3 MEDIA & GENERAL PUBLIC 14
7.4 THIRD-PARTY SERVICE PROVIDERS 14
7.5 REGULATORS 14
8 GOVERNANCE 15
8.1 INTERNAL AUDIT 15

1 PURPOSE

This document outlines the Company's Business Continuity Management (BCM) procedures with the aim to provide clients and external persons a greater understanding how the Company manages business continuity risks.

1.1 SCOPE

The Company's BCM includes the Business Continuity Plan (BCP) and Disaster Recovery (DR) for MarketAxess Holdings Inc. (MAH) and its subsidiary entities.

1.2 DOCUMENT MAINTENANCE DISCLOSURE

This document contains the latest view of the Company's BCM and test results. The Company will review and update this document as it deems appropriate. Typically, this will be to incorporate the latest annual test cycle and results, or if there have been any significant changes to the Company's BCM process.

2 BUSINESS CONTINUITY MANAGEMENT

2.1 APPROACH

The Company's BCM procedures assist the Company in appropriately responding to business interruptions in relation to loss of access to people, facilities, technology, or third-party service providers and in restoring the services provided to its clients as soon as reasonably possible.

As part of its business continuity efforts, the Company has developed detailed BIAs (Business Impact Analysis) for all core departments together with a crisis management playbook which are supported by detailed departmental BCP playbooks.

These are collectively designed to help the Company enact its business continuity procedures following a major business interruption such as any anticipated high-profile local events, natural disasters or other unanticipated events (such as a power failure, security breach) that disrupts the Company's business for an extended period.

In the event of a major business interruption, the Company will initiate its business continuity procedures which include:

- Initiation of the crisis management playbook and open relevant communication channels. The business impact analyses are referenced to assess the potential impact of the business interruption.
- Evaluation of the incident to assess the client/third-party impact and provide relevant and appropriate communication to clients and other relevant third parties.
- Implementation of the response plans detailed in the BCP playbooks.
- Implementation of the necessary and appropriate contingency plans for the recovery and resumption of services following the loss or impairment of people, process, technology or critical third-party vendors.
- Evaluation of any regulatory impact.

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

- Data recovery procedures invoked.
- Restoration of critical systems and processes (e.g., regulatory reporting).
- Financial and operational impact assessments.
- Reinstate remote working for staff.
- Assess and invoke critical suppliers' and third-party vendors' contingency plans.

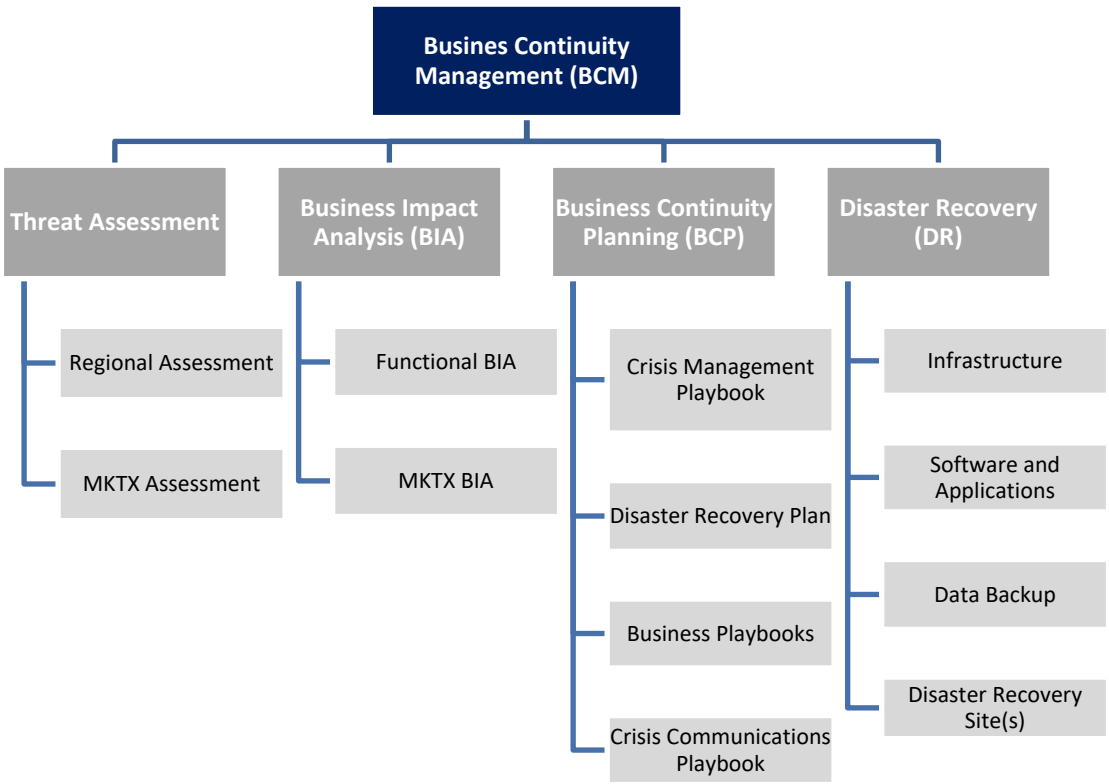
2.2 BCM Framework

The Company has adopted a BCM 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 Business Impact Analyses.

The result of the BCM framework is a documented process that outlines how the Company will respond to events that result in the loss or impairment of people, facilities, technology, or third-party vendors.

Below diagram provides a high-level structural overview of the Company's BCM framework.



2.3 Crisis Management Strategy

The Company utilizes a structured approach to respond to and recover from any crisis, regardless of the severity of the incident, and locations or business units impacted by the incident. This staged approach is comprised of the following four phases:

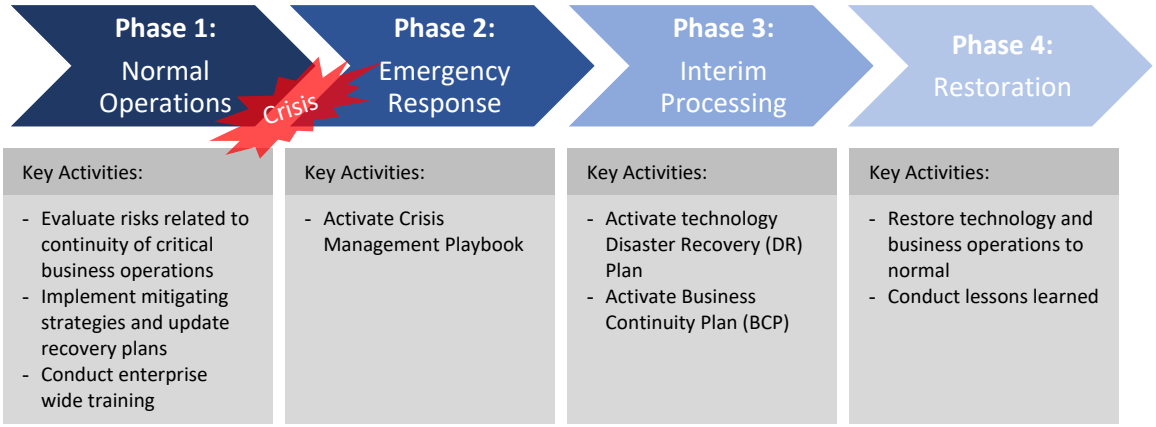
- **Phase 1: Normal Operations** – this phase is ongoing until business interruption occurs. During this phase, the operations are normal; however, preparation efforts are conducted to evaluate risks related to continuity of critical business operations and to implement mitigation plans.

- **Phase 2: Emergency Response** – this phase begins immediately after the occurrence of a crisis event and continues until the situation is stabilised. The goal during this phase is to minimize injuries and loss of life and to manage and contain the crisis.

- **Phase 3: Interim Processing** – this phase begins immediately after a crisis event is declared and continues until business is restored back to normal operations. During this phase, temporary procedures may be implemented to resume critical business processes as quickly as possible.

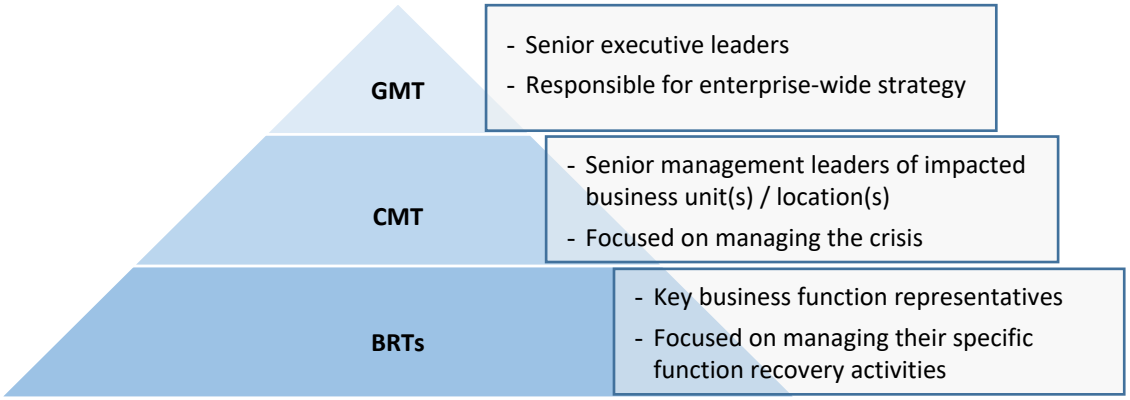
- **Phase 4: Restoration** – this phase begins after critical services are recovered to acceptable service levels. The goal during this phase is to return the organization back to normal business operations.

The following diagram outlines key activities performed during each stage of the recovery process:



2.4 Recovery Team Structure

The Company's recovery team structure is comprised of three primary response teams, including the Global Management Team (GMT), Crisis Management Team (CMT), and Business Recovery Teams (BRTs). These three interactive teams will carry out a centralized, enterprise-wide response to a crisis event with local ownership of recovery activities at each office and data center locations.



Global Management Team (GMT)
The GMT is comprised of senior executive leaders and is responsible for the enterprise-wide strategic decision-making activities. This team would only be activated during the most severe types of crisis events. The GMT is appropriately informed during less impactful events.

Crisis Management Team (CMT)
The CMT Communication Leader (or their representative) is responsible for communicating business interruption based on the nature, severity and urgency of the interruption. CMT members represent senior leaders from the core corporate functions. This team provides corporate support to local and Business Recovery Teams and is led by CMT Lead(s) from each impacted location.

Business Recovery Team (BRT)
The BRT represent senior leaders from individual business units at specific office locations. Each Business Unit CMT member is responsible for managing the crisis for their business unit across their geographical presence. If a crisis impacts multiple business units and/or multiple locations, then the Business Unit CMT member from each impacted group will be involved in managing and directing the crisis response.

3 BUSINESS CONTINUITY PLAN

The Company's BCP focuses on the availability or impact to the Company's office site, people and operational activities.

3.1 Crisis Management Playbook

The Company has created a Crisis Management Playbook (CMP) which sets out the BCP requirements for MarketAxess Holdings Inc ('the Company', which incorporates the Company along with its subsidiaries).

The CMP is a central document that provides a single source for each entity within the Company to understand the Company's:

- Crisis Management framework
- The construction of the CMT and their related roles and responsibilities
- Procedures for identifying and declaring a crisis event

- Checklist of activities for the CMT to address the most critical recovery issues
- Communications plan to disseminate information to customers, employees, third-party service providers, regulators and the media

The goal of the CMP is to pre-establish a response and recovery procedures to:

- Minimize injuries or loss of life
- Effectively identify, assess, manage, monitor and contain the business disruption event
- Focus on the most critical business activities
- Restore communication with customers, third-party vendors, regulators and the public

3.2 Business Impact Analysis

A Business Impact Analysis (BIA) is conducted for each department, e.g., Finance, Infrastructure, Client Services.

The BIA process is 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 including data, equipment and other infrastructure required, and the recovery time objectives and recovery point objectives.

The BIA is an annual assessment that informs recovery priorities (people, process systems, and third parties) and forms part of the departmental playbooks / plans.

3.3 Detailed Playbook/Plans

An actionable BCP "Playbook" has been developed for each department outlining how that team will operate during a business interruption.

The playbook contains information such as (but not limited to):

- What the function must do in the event of a crisis
- Key processes, workflows and checklists
- Minimum number of staff to maintain operations during a crisis
- Key contacts (internal staff, third-party vendors, regulators)
- Key applications and systems

3.4 Offsite Locations

The Company has prepared for events resulting in the loss of physical facilities. Processes and staff would operate through either working remotely, or use of alterative offices.

Staff

Staff members will be required to work from alternative offices (where possible) and/or work remotely. The Company has made the following assumptions:

- All staff members are equipped with laptop allowing them to work remotely securely.

Additional Considerations

- The Company has capabilities to utilize corporate resources and facilities in other geographical locations (e.g., New York City, London, Amsterdam, Hong Kong, Singapore), such as:
  - Staff
  - Telephone services

Having resources and facilities in multiple geographical locations reduces the impact of local crisis events and single points of failure.

3.5 Third-Party Service Providers

We have a process in place to identify critical Third-Party service providers which requires them to periodically pass through a due diligence process undertaken by several functions, including but not limited to our Legal, Finance, Compliance, Risk and Information Security departments. This due diligence process includes a review of the Third-Parties business continuity process and controls. Performance monitoring of critical Third-Parties is conducted throughout the year.

4 DISASTER RECOVERY

Disaster Recovery (DR) focuses on the availability or impact to the Company's data centers, systems and servers.

4.1 Data Centers

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

- US: Secaucus, New Jersey - Primary Production Data Center provided by Equinix
- US: Ashburn, Virginia - Backup Data Center provided by Equinix
- EU: Dublin, Ireland (IE) - Primary Cloud Data Center provided by AWS
- EU: Frankfurt, Germany (DE) - Backup Cloud Data Center provided by AWS

US data centers are located over 200 miles (~320 km) apart, and EU data centres are over 850 miles (~1350 km) apart to minimize simultaneous risk to power or physical disasters.

The data centers are setup in a warm-standby model, and in the event of a full primary site failure we can activate the services from the secondary site. The data centers have asynchronous replication in place.

4.1.1 Recovery Times

The Company 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

The Recovery Point Objective (RPO) represents the amount of data (in minutes) that can be lost before there is unacceptable impact to the end-users. The RPO is **0 seconds** (orderly winddown).

Procedures have been developed and put in place which will help minimize the impact of failover to the disaster recovery site. Any failover is considered extremely rare due to the resilience and fault tolerance built into the Company's data centers and applications.

Recovery Time Objective

The Recovery Time Objective (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 RTO stands at **2 hours** for Trading Services and **4 hours** for Post Trade Services.

4.2 Systems and Servers

Business function system and application criticality is identified and assessed as part of the BIA. The BIA is used to determine the DR recovery requirements and prioritization. Testing is conducted to ensure that the prioritization is accurate and ensures that the Company can operate as expected in a timely manner.

4.3 Backup Overview

The Company conducts daily, weekly and monthly backups which are maintained for a minimum of **7 years** or pursuant to regional applicable law. The restoration of these backups is conducted as required on an ad-hoc basis.

4.4 Crisis Management Scenarios

The Company has conducted a formal risk assessment to identify the most likely types of crisis that would invoke BCM. The below risk scenarios have been identified by the Company as potential crisis trigger points. To help ensure timely notification to and activation of the CMT, the Company has designated BRTs with the responsibility of escalating specific trigger points.

Ref	Threat	Threat Description
Natural Hazards		
1	Earthquake	Earthquakes strike suddenly, without warning. Ground shaking from earthquakes can collapse buildings and bridges, disrupt gas, electric, and phone services.
2	Flooding	Extreme weather may result in flooded facilities, damage to premises and equipment, power disruption, and inability of employees to access facilities.
4	Fire (Internal)	Internal fire may result in injured employees, damaged facilities, and inability to access the primary facility for an extended period.
5	Extreme Heat	A heat wave is an extended period of extreme heat and is often accompanied by high humidity. These conditions can be dangerous to the health and may cause heat-induced occupational illnesses, injuries, and reduced productivity in a hot work environment.
6	Tornadoes	Wind speeds more than 150 miles per hour, about 250 feet across and a few miles wide that usually last no more than a few minutes. These storms can result in major facility damage to complete destruction and death, with little warning.
7	Wildfires (External)	Uncontrolled fire in an area of combustible vegetation that typically occurs in the countryside and can cause extensive damage, both to property and human life. May result in injured employees, damaged facilities, and inability to access the primary facility.
8	Drought	Excessive dry weather affecting the water supply.
9	Hurricane / Typhoon	Storms over a large region with winds that exceed 64 knots and heavy rains that may result in substantial damages to facilities, associate injuries and death, or significant flooding.
10	Landslide	Significant collapse of mud, rockslides, and debris flows, causing significant property damage and possible death.
11	Severe Winter Weather	Cold temperatures, snow and ice may result in damaging and deadly storms.
12	Thunderstorm & Lightning	Electrical storms causing sporadic power outages.
13	Pandemic	An epidemic of infectious disease that has spread through human populations across a large region.
Technology		
14	Backup/ Replication Failure	Data backup failure or loss of backup media.
15	Computer Viruses	Viruses affecting computers and servers leading to downtime and data loss.
16	Capacity Shortfalls	Capacity constraints causing reliability and availability issues.
17	Power Failure	Loss of key systems and an inability to continue business processes.

Ref	Threat	Threat Description
18	Network Intrusion	External activity resulting in denial of service, confidential data loss, and significant network and system outages.
19	System/ Infrastructure Failure	Catastrophic technology failure, rendering systems unavailable for an extended time period.
20	Telecomm Failure	Loss of external or internal communication methods with customers, suppliers, and internally.
21	Ancillary Equipment Failure	Short-term or long-term failure of HVAC, water, and/or plumbing.
22	Data Theft	Compromise of sensitive data such as customer or employee personal information(e.g., credit card numbers).
23	Third-Party	Loss of a third-party impacting the provision of services
Man-Made		
23	Physical Equipment Theft	Compromise of physical assets (i.e., laptops, PCs, servers, etc.) leading to significant data or proprietary information loss as well as financial implications.
24	Terrorist Attack	A surprise attack against civilians resulting in significant property damage and/or loss of life.
25	Aircraft Crash	A private or commercial aircraft crash resulting in significant property damage and loss of life.
26	Mass Public Gatherings	Labor/Political disputes – protests, demonstrations, rallies, marches, strikes and similar gatherings are means for a mass of people to crowd high traffic locations and may result in inability of staff to report to work.
27	Building Defects	Building collapse resulting in loss of life and property damage.
28	Explosion	Intentional or accidental explosion resulting in loss of life and property damage.
30	Sabotage/ Vandalism	Deliberate and destructive actions caused by internal or external entities.
31	Toxic Contaminations	Release of hazardous chemicals.
32	Neighboring Business Risk	High risk businesses are located nearby that may cause disruptions to business operations.
33	Cyber Security	Cyber security attack.
34	War	Armed conflict between the armed forces of states or between governmental forces and armed groups

5 PANDEMIC (E.G.: COVID-19)

The Company's control framework is designed with the ability for staff to work remotely, and where necessary to increase utilization of global infrastructure to support local requirements, subject to and in accordance with our existing intra-group outsourcing agreements. MarketAxess continues to monitor local government and global health organization guidance and aims to act in accordance with such recommendations in relation to staff welfare, client services, customer support and communications.

The Company's current assessment is that MarketAxess does not anticipate significant operational impact or deviation from the product offering and client service levels offered in the course of normal business. MarketAxess' operational resilience is underpinned by three pillars of resourcing/planning, (1) remote working policy, (2) cross training strategy, and (3) a model of global operational inter-operability/support.

In all offices, travel restrictions for staff, and strict office access MKTX implemented a work from home strategy for its Global employees. This has been done in combination with increased local sanitation provision policy. We have since adopted a hybrid working model.

We have clear guidelines for self-isolation in the event of suspected exposure or symptomatic presentation.

6 TESTING, AWARENESS AND DOCUMENTATION

The Company is dedicated to its BCM program which is supported by maintenance of its continuity documentation, keeping its employees trained and aware with the latest information, and performing multiple tests throughout the year. The goal is to ensure that the Company is supported by a functional BCM program which optimizes our position to prevent or react to a crisis.

BCP Sites and Systems
At a minimum, once per year a disaster recovery test and an office availability test is performed. The disaster recovery test is centered around unavailability of the data center and applications.

The tests are aimed to ensure that the systems are accessible, recover as expected within a reasonable timeframe, and that the business end-to-end operations are fully functional working remotely.

The Company also participates in cross-industry wide Business Continuity exercises, such as the ones organized by SIFMA.

Employee Awareness
The Company performs a BCP tabletop test exercise with all departments to assist management in evaluating the effectiveness of the BCP plans and the Company's readiness to implement the plans during a business disruption using realistic scenarios.

Documents
Documents are updated or reaffirmed at least once per annum or when there is significant change to the business or BCM requirements.

All continuity plans are stored in multiple locations to mitigate any single point of failure. Documents are stored in the following locations:

1. The Company's intranet site
2. A secure independent web-based application
3. Secure Risk folders on the internal network

6.1 2024 Results

There have been no significant findings or failures identified in the Company's annual testing program. Below is a list of the core testing performed throughout 2024.

Ref	Category	Testing, Updates and Awareness Type	Date	Comments
1.	Pandemic Preparations	All sites	Continuous	**Successful** All office locations are prepared and maintained to necessary standards for when employees are able to return.
2.	Communication	Emergency notification to staff	Feb & Oct 2024	**Successful** No significant findings identified
3.	DR Tests	Data Centers	Sept, Oct 2024	**Successful** Recovered within RTO and RPO
4.		Remote Access Tests and VPN Tests	Multiple per year	
5.	Awareness	Training and Awareness	Multiple per year	**Successful**
6.		Round table discussions / scenarios	Multiple per year	
7.		New hire/starter training and awareness program	Multiple per year	
8.	Documents	Crisis Management Playbook (currently being upgraded to broaden scope)	Q1 2025	**Successful** Maintained and updated by Risk
9.		Business Continuity (Playbooks, Runbooks, BIAs)	Throughout the year	**Successful** Maintained and update by the throughout 2024
10.		Communication Plan (currently being upgraded to broaden scope)	Q1 2025	**In progress**
11.	Audit	BCM Internal Audit	June 2024	**Successful** No significant findings identified

7 COMMUNICATION

The Company has predefined processes to communicate with several audience groups during a crisis event. These groups include (but are not limited to) employees, clients, critical third-party service providers, investors, regulators and the public.

7.1 EMPLOYEE COMMUNICATIONS

The Company has established several mechanisms to alert employees of a business interruption and provide additional instructions and information related to the event. Primary methods for all employees include:

- Emails
- Text messages via mass communication system (external hosted system)

Additionally, designated business continuity hotlines would be opened and periodically updated for Client Service Management and Production Support.

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

If the above independent systems are unavailable, alternative methods will be used, such as (but not limited to) corporate and personal emails, mobile phones and internal intranet postings.

7.2 CLIENT COMMUNICATIONS

The Client Service Management team and/or a designated Sales representative are the designated client facing personnel to be responsible for direct communication with clients. These individuals will work closely with the CMT to ensure that accurate and timely messages are communicated to customers. Communication methods will largely depend on the type of crisis and how many customers are affected. In general, secure lines of communication with clients (corporate email) are preferred over non-secure communication methods (e.g., cell phone, website).

Client Service Management and the Sales representatives maintain a readily available list of necessary client contact details.

7.3 MEDIA & GENERAL PUBLIC

Communications with the media and the general public are handled by the CMT Communications Leader or its Representative and where necessary, the public facing websites and switchboards will be updated periodically.

7.4 THIRD-PARTY SERVICE PROVIDERS

BRT leads and/or Third-Party Relationship Managers are responsible for contacting and communicating with critical third-party service providers to request support in the recovery efforts. Third-party dependencies are documented in both the BCP Playbooks and DR documents for each business unit.

7.5 REGULATORS

Communications with the regulator(s) are handled by the CMT Legal/Compliance Leader.

8 GOVERNANCE

The Company has in place relevant teams and assigned designated leads who are responsible for the governance of BCM within their sphere of responsibility. The overarching BCM governance is managed by the Risk and Technology functions, for BCP and DR respectively. BCM updates (including test results) are communicated at several levels of the Company's governance structure (including the Company's Board Risk Committee).

8.1 INTERNAL AUDIT

The Company's Internal Audit department periodically audits the BCM. The most recent audit of the Company's BCM was conducted in Q2 2024 and had no significant findings.