Business Continuity Plan Summary

The "Business Continuity Plan Summary" document summarizes the Business Continuity Strategy and Tactics and applies to the businesses of **Cantor Fitzgerald, BGC Partners, GFI Group, Newmark Knight Frank, CastleOak Securities, CF Secured, R. P. Martin, Sunrise Brokers,** all subsidiaries and other entities ("**the Group**") to which Cantor Fitzgerald Securities and Tower Bridge International Services L.P., respectively, supply BCM services pursuant to intercompany service level agreements.

AUTHOR (S): ANI PIRA, ANDREAS BRYANT

AUTHORIZED BY: BUSINESS CONTINUITY MANAGEMENT

DATE: JAN 2019

VERSION: 3

This is the 2019 "Public" version of the firm's strategic / tactical level Business Continuity Plan.

This version of the plan specifically excludes detailed and confidential information that is not generally shared with third parties. Any party requiring further information should submit a justification / business reason for such additional data via request to the Cantor Fitzgerald Securities' Business Continuity Management Office, BCM@Cantor.com

Business Continuity Management Framework

The Group operates across a substantial number of office locations globally. Business Continuity Management is delivered via respective regional offices in New York and London.

- Ani Pira, Global Head of Business Continuity - Americas
    - 199 Water St., Eighteenth Fl., New York, NY 10038
- Andreas Bryant, Regional Head of Business Continuity - EMEA & Asia PAC
    - 1 Churchill Place, Canary Wharf, London, E14 5RD

Day to day executive oversight of the program is through the Cantor Fitzgerald Securities' Chief Administrative Officer. Direction of the program follows the Business Continuity Policy, which is updated based on material changes to the business and reviewed annually by the Business Continuity Management Office and Group Senior Management. The framework is aligned with, current global and financial markets benchmarks, best practices and standards including FINRA Rule 4370, ISO 22301, the Global Good Practice Guidelines of the Business Continuity Institute and Disaster Recovery Institute International.

Our regulated businesses also follow guidance and direction issued by their relevant market supervisory requirements.

Scenarios

Our plans address the following high-level scenarios:

- Building Event – all or part of the facility is unavailable for use.
    - A building might be an office location or a data center
    - The cause of the event is immaterial at the time of an incident but might be fire, flood, explosion, power failure etc.
- Technology Event – significant non-availability computer and / or communications infrastructure.
    - In the context of our office locations, as our IT services and data are delivered from a network of central data centers in the USA, UK and Asia, a technology event is most likely to be an impact upon the network infrastructure.
    - In the context of a data center, such events are likely to be the catastrophic loss of function of multiple IT systems and services. The IT Disaster Recovery Plan and IT Group BCP address the response to such events
- People Event – significant non-availability of staff required to undertake critical business operations.

Our plans are designed to provide the required response to address a "worst case scenario" and are sufficiently flexible and scalable that they will support events of lesser magnitude.

Delivering Assurance

We use a number of strategies to ensure that our plans and preparations collectively and continuously deliver the level of functional assurance and "recoverability" that is necessary to:

- Satisfy our obligations and protect the interests of our customers, regulators and other key stakeholders (including our staff);
- Protect our reputation and brand value;
- Ensure the ongoing viability of our business and operations.

Those strategies include:

- Generating and communicating awareness through provision of on-boarding data to new staff and a variety of communications that regularly refresh communication with existing staff;
- Testing of mass communication strategies and technologies;
- BCP and IT recovery exercises and tests – ensuring that all critical components of our framework are tested at least annually (and more frequently where the criticality of the team or recovery element so depends);
- IT recovery testing conducted within the Business Continuity framework generally falls into two approaches:
    - Testing of the availability, resilience and / or recovery concepts associated with a specific platform where such testing forms part of a specific contractual or regulatory obligation; or
    - Full data center isolation testing – in which the goal is to simulate the total loss of a data center and, in partnership with our business teams, confirm that the performance and functionality of the recovery environment meets the recovery and recovery time objectives (RTOs) identified for each of our businesses.

Continuity and Recovery Strategies – BCP / Work Area

The firm's aim, following a disruptive incident, is to meet all contractually or regulatory binding obligations within the parameters set out in associated agreements. Thereafter our general recovery objectives in the event of denial of access to our normal work environment are as follows:

- "Primary" front office and associated supporting middle and back office functions (e.g. transaction processing, confirmation, settlement, etc.) to be resumed within four hours of an interruption. To support this goal we maintain:
    - Work area recovery sites in strategic locations that are fully equipped, maintained and tested so as to ensure they provide a user-ready environment when needed;
    - Technical strategies, including use of virtual desktop profiles, that support speed, efficiency and multiple accessibility options – including remote access / home-working where appropriate;
    - Our extensive branch office network provides access to workspace, data connectivity and voice communications for many functions that are self-sufficient in recovery and do not depend upon centralized recovery support.
    - More immediately critical activities resumed through use of contingency arrangements appropriate to the function, such as alternative ways of working (e.g. manual work-arounds) where a process must be restored more quickly than it might be possible to restore the normal processing infrastructure.

Continuity and Recovery Strategies – IT

The IT Group maintains a resilient IT infrastructure that protects the firm's most critical technology and data requirements using:

- IT Service delivery models that require components to be distributed across multiple data centres (DCs) separated by distance, utility grid and risk and in such a way as to provide extensive redundancy and high availability.
- High availability or back-up and restore capabilities that are appropriate to RTOs required to meet customer or regulatory obligations for the firm's most critical IT systems and services;

- Diverse network and communications routing – ensuring that disruption or failure of one route results in the automatic re-routing of voice and data networks via another part of the infrastructure.

Procedures for fail-over / activation of the associated systems and services are set out as part of BGC's Group IT procedures and cross-referenced to IT Disaster Recovery Plans / Teams as appropriate.

Operational testing of IT Disaster Recovery resources and infrastructure takes place routinely as an extension of IT maintenance and change management procedures.

An ongoing schedule of Data Centre isolation tests enables us to simulate and exercise response to the loss of a Data Centre ensuring that our ability to maintain or restore our most immediately critical services shall be accomplished within our associated RTOs. All critical services are implemented using concepts that ensure zero data loss.

Additional testing to ensure the integration of IT recovery and business continuity is managed and maintained as part of the firm's overall Business Continuity Management Program / System which also includes staff familiarization and awareness training exercises that ensure efficiency in deployment when needed.

Incident Response and Plan Activation

BCM executes a "tiered" incident response strategy defined by scale and relative importance of each location and by the severity of impact of an incident.

- Our incident response process determines how and by whom the response will be managed and escalated. As an illustration
    - Events that have either zero or only very minor impact on our operations, are addressed by normal operational management – although details of the event may be recorded and submitted for further review as part of our general risk management procedures
    - Events that result in harm to personnel and / or directly affect the conduct of operations will trigger a formal incident response and escalation in accordance with specific criteria.
- We maintain regularly trained and exercised tactical incident response teams at each of our major locations and, groups with strategic oversight responsibilities at a regional and / or global business level.

Crisis Notification and Communication

BCM maintains, and regularly tests, our mass communication tool that enables us to quickly and easily communicate with and direct our staff in the event of an incident. The database associated with the tool enables us to select staff generally within a geographic area or specifically by office location or, in certain cases, by selected functional group.

As a general rule the aim of our plan framework is the continued delivery of our key customer services and that any constraint upon normal operations should be largely transparent to our customers – consequently, provided our recovery plans work as expected following an incident, we would not expect to contact customers to advise of any outage. In exceptional circumstances where an event results in measureable deterioration of service we will communicate directly with our customers and other stakeholders to advise of any change in procedures or expected transaction processing while we work to restore normal processing capabilities.