Group Business Continuity Plan Summary

The “Business Continuity Plan Summary” document summarizes the Business Continuity Strategy and Tactics, and applies to the businesses of BGC Group, Cantor Fitzgerald, GFI Group, Fenics, Newmark, all subsidiaries, and other entities (“the Group”) to which Cantor Fitzgerald Securities and Tower Bridge International Services L.P., respectively, supply Business Continuity Management services pursuant to intercompany service level agreements.

AUTHOR(S): ANI PIRA, MILENA MANEVA

AUTHORIZED BY: BUSINESS CONTINUITY MANAGEMENT

DATE: JANUARY 2024

VERSION: 6

This is the 2024 “Public” version of the Group’s strategic and 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 Group’s Business Continuity Management.

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.

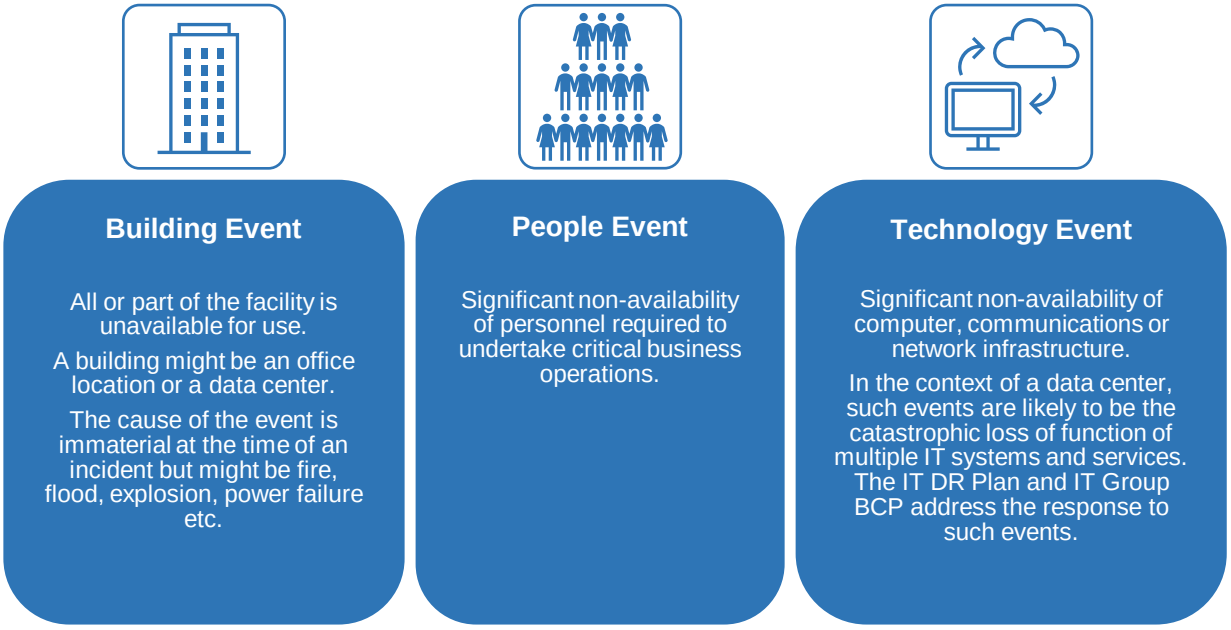
- **Ani Pira**, Global Head of Business Continuity Management Americas / APAC
  – 199 Water St., Nineteenth Fl., New York, NY 10038
- **Milena Maneva**, Head of Business Continuity & Resilience, EMEA
  – 5 Churchill Place, Canary Wharf, London, E14 5HU

Day to day executive oversight of the program is through the Cantor Fitzgerald Securities' Chief Administrative Officer. The 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 and Group Senior Management.

Our methodology and framework align with globally recognised continuity and resilience standards, best practices and financial markets benchmarks including FINRA Rule 4370, ISO 22301, FCA's Operational Resilience Policy requirements. Our regulated businesses also follow guidance and direction issued by their relevant market supervisory requirements.

Scenarios

Our business continuity and resilience 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. Our plans address the following high-level scenarios:



Delivering Assurance

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

- Satisfy our obligations and protect the interests of our customers, regulators, and other key stakeholders (including our personnel).
- Protect our reputation and brand value.
- Improve the overall Group's resiliency.
- Ensure the ongoing viability of our business and operations.

Those strategies include:

- Generating and communicating awareness through provision of on-boarding data to new personnel and a variety of communications that regularly refresh communication with existing personnel.
- Testing of mass communication strategies and technologies.
- BCP, Operational Resilience and IT DR 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).
- Operational Resilience testing to assess Group's ability to remain within its impact tolerance for each of its important business services in the event of a severe but plausible disruption of its operations.
- IT DR 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.
  - 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 - Business Continuity

The Group's aim, following a disruptive incident, is to meet all contractual 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 business as usual (BAU) operations and to be resumed within four hours of an interruption are as follows:

- Primary Front Office, and
- Middle and Back Office supporting functions.

To support this goal, we maintain:

- **Workplace Recovery (WPR)** sites in strategic locations that are fully equipped, maintained, and tested to ensure they provide a user-ready environment when needed.
- **Remote Access / Home Working** - technical strategies, including use of virtual desktop profiles, that support speed, efficiency, and multiple accessibility options.
- **Other Offices / Process Transfers** - 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.
- **Contingency Arrangements** - more immediately critical activities resumed through use of contingency arrangements appropriate to the function, such as alternative ways of working (e.g., manual workarounds) where a process must be restored more quickly than it might be possible to restore the normal processing infrastructure.

Continuity and Recovery Strategies - IT DR

IT Disaster Recovery is separately managed by the IT Group, who maintain a resilient IT infrastructure that protects the Group's most critical technology and data requirements using:

- IT Service delivery models that require components to be distributed across multiple data centers (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 Group'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 failover / activation of the associated systems and services are set out as part of the Group's IT procedures and cross-referenced to Technology Recovery Action 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 center isolation tests enable us to simulate and exercise response to the loss of a data center ensuring that our ability to maintain or restore our most immediately critical services will be accomplished within our associated RTOs. All critical services are implemented using concepts that ensure zero data loss.

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 matrix 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 must be recorded and submitted for further review in line with Risk Management policies and procedures.

  → Events that result in harm to personnel and / or directly affect the conduct of normal business operations will trigger a formal incident response and escalation.

- 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 notification system that enables us to communicate with our personnel quickly and efficiently in the event of an incident. The database associated with the tool enables us to select personnel within a geographic area or specifically by office location or, in certain cases, by selected functional group. The Group will provide regulators with contact information for emergency contact persons through the appropriate methods.

The aim of our communication plan framework for BCM and operational resiliency is the management of the communications during an incident and the continued delivery of our key customer services. Any constraint upon normal business 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 them of any outage. In exceptional circumstances where an event results in measurable 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.