Group Business Continuity Plan Summary

The “Business Continuity Plan Summary” document summarizes the Group’s Business Continuity and Resilience Strategy and Tactics, and applies to the businesses of Cantor Fitzgerald, BGC Group, GFI Group, Newmark, including 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 (BCM)
Latest Version	Version 8
Last Updated	December 2025

This is the public version of the Group’s Business Continuity Plan, which outlines our strategic and tactical approaches. This version supersedes all previous versions and may be shared externally.

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
  - 199 Water St., Eighteenth 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 LP Chief Financial 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, Digital Operational Resilience Act (DORA), CFTC ORF, 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:

PEOPLE EVENT

Significant non-availability or loss of personnel required to undertake critical or important business operations.

BUILDING EVENT

A building event occurs when a facility, such as an office location or data center, becomes partially or fully inaccessible or unavailable. While the cause of the event is secondary during the incident, it may include scenarios such as fire, flood, explosion, or power failure.

TECHNOLOGY ICT-RELATED EVENT

An Information and Communications Technology (ICT) event or a series of linked unplanned events that compromise the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the Firm.

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.
- Business Continuity 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 IT service or critical or important function where such testing forms part of a specific contractual or regulatory obligation.
  - Datacenter isolation testing – in which the goal is to simulate the total loss of a datacenter 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) and Recovery Point Objectives (RPOs) identified for our critical or important functions and services.

Continuity and Recovery Strategies - Business Continuity

In the event of a disruptive incident, the Group is dedicated to fulfilling all contractual and regulatory obligations outlined in relevant agreements. If access to standard business operations (BAU) is compromised, our top priority is to restore Critical or Important Functions (CIF) and Important Business Services (IBS) within a recovery time objective of zero to four hours. This commitment encompasses mission-critical operations and services across our Front Office, Middle Office, and Back Office support functions.

To support this goal, we maintain the following:

- **Workplace Recovery (WPR)**: Dedicated sites in strategic locations that are fully equipped, maintained, and regularly tested to ensure they provide a user-ready environment when needed.
- **Remote Access / Home Working**: Technical solutions, such as virtual desktop profiles, designed to enable rapid, efficient access and support a range of connectivity options.
- **Other Offices / Process Transfers**: A comprehensive network of branch offices that offer workspace, data connectivity, and voice communication capabilities. These offices can support many functions independently and do not rely on centralised recovery support.
- **Contingency Arrangements**: Critical business services and functions are supported through contingency measures tailored to each function. These may include alternative methods of operation, such as manual workarounds, for processes that need to be restored faster than the normal processing infrastructure allows.

Continuity and Recovery Strategies - IT DR / IT SM

The IT Group independently manages IT Disaster Recovery (IT DR) and IT Service Management (IT SM) to maintain a robust and resilient IT infrastructure. This infrastructure safeguards the Group's most critical technology and data needs through the following measures:

- **Distributed IT Service Delivery Models:** Key components are strategically spread across multiple data centres (DCs) that are geographically distant and separated by utility grids and risk factors, providing extensive redundancy and high availability.

- **High Availability and Backup Solutions:** Comprehensive backup and restoration capabilities align with the required Recovery Time Objectives (RTOs) to meet customer and regulatory obligations for the Group's most critical IT systems and services.

- **Diverse Network and Communication Routing:** Redundant routing ensures that any disruption or failure in one route triggers an automatic rerouting of voice and data traffic through alternative infrastructure paths.

Failover and activation procedures for related systems and services are detailed in the Group's IT DR procedures and referenced in the ICT Business Continuity Plans (aka Technology Recovery Action Plans or TRAPs) for critical IT services. Routine operational testing of IT DR resources and infrastructure is integrated with IT maintenance and Change Management protocols.

Regular data centre isolation tests allow the Group to simulate and exercise responses to potential data centre outages, ensuring that our most critical services can be maintained or restored within the specified RTOs. All critical services are designed to prevent data loss, using advanced methods to ensure continuity.

Incident Response and Plan Activation

BCM executes a "tiered" incident response strategy defined by scale, criticality of each location, and the severity of impact of an incident. Our incident response matrix determines how and by whom the response will be managed and escalated.

The Incident Management Team (IMT) is composed of a group of individuals across the region who are responsible for developing and implementing a comprehensive plan for responding to a disruptive incident. The team consists of a core group of decision-makers from each location in the region who are trained in incident management and prepared to respond to any situation. The IMT is the primary group that assesses an incident that might affect the Group's ability to conduct normal business.

The **Incident Response Teams (IRT)** and the **Global Technology Response Team (TRT)** support the IMT in the execution of the response strategy and enforce the decisions made by the IMT. Events that concurrently affect more than one office location in a major city will require collaboration and cooperation between the IRT's of each facility – this will be coordinated by the BC Management office. Additional staff may be required in scenarios where special expertise is required or a larger group is needed to undertake the tasks necessitated by the incident.

Tiered Response Overview:

Tier	Description / Criteria	Impact / Scope	Response	Examples
Tier 1 – Critical	Severe incidents threatening business continuity, safety, or regulatory compliance.	Severe impact; cross-organizational disruption; legal or reputational implications.	Immediate full-scale IRG response activation; senior leadership and stakeholders involved.	Cyberattack on core systems, major data breach, natural disaster affecting operations, critical facility security incident
Tier 2 – Major	Significant incidents impacting critical systems or multiple departments, offices.	High operational impact; risk to data, compliance, or reputation.	Full IMT & IRT team activation; management informed; formal plan execution.	Multi-department service outage. Widespread malware outbreak, critical system failure.
Tier 3 – Medium	Incidents affecting multiple users or systems but are contained.	Moderate impact; partial service disruption.	Escalate to regional IRT and/or local contacts may trigger partial incident response plan.	Network slowdown, partial service outage, ransomware detected but contained.
Tier 4 – Minor	Minor issues that do not significantly affect operations.	Localized, minimal impact; limited to one system or team.	Handled by first-level support or IRT; no formal plan activation.	Single workstation malware, minor system glitch, small user error.

Operational Guidance:

- Events with zero or minor impact are managed through standard operational processes, with details recorded for risk management review.
- Events that affect personnel safety or disrupt normal operations trigger a formal incident response and escalation according to the matrix above.
- Tactical incident response teams at major locations handle immediate mitigation, while regional or global oversight groups provide strategic guidance and coordination.
- Communication methods are selected based on severity, ensuring rapid awareness and effective resolution.

For critical incidents, the priority is to restore essential business functions as quickly as practicable. Lower-tier incidents are managed through standard operational processes, with escalation if conditions worsen.

All incidents, including minor events, are recorded for review and continuous improvement. The BCP and its tiered matrix are regularly tested, updated, and exercised to ensure effectiveness and alignment with evolving business needs.

Communication During Emergencies, Crises, and Incidents

Depending on incident severity, notifications may be internal (site management and operational teams), management-level (regional or global coordinators), or broader (executive leadership and relevant stakeholders). The method of communication is selected to ensure rapid awareness and effective coordination. The Group's Business Continuity Management (BCM) team maintains and regularly tests a notification system to enable rapid and effective communication with personnel during incidents. This system allows for targeted notifications to individuals based on geographic location, office site, or specific functional group as needed. BCM utilizes internal and external contact systems and methods to respond to crises and incidents across various scenarios.

The communication plan framework for BCM and operational resilience is designed to manage all aspects of incident-related communication, including internal communications, while ensuring the uninterrupted delivery of key customer services. Our objective is for any disruption to normal business operations to remain largely transparent to customers. Therefore, if recovery plans function as intended, we do not anticipate needing to inform customers of an outage.

However, in exceptional cases where a significant deterioration in service occurs, we will directly communicate with customers, regulators, and other stakeholders. This communication will include any changes to procedures or expected transaction processing timelines as we work to restore normal service.

Key aspects of our communication strategy

The following key aspects of our communication strategy are outlined in the Incident Response Guide (IRG) and include, but are not limited to:

- **Internal Communication:** During an incident, effective internal communication is critical. The BCM team will ensure that all personnel are informed about the situation, including updates on incident status, recovery efforts, and any changes to operational procedures. Clear channels will be established to facilitate this communication, ensuring that all employees receive timely and accurate information.

- **Governance and Reporting Lines:** We uphold robust internal governance and controls for incident management. This framework ensures the escalation of major ICT-related incidents to senior management and includes a process for coordinating and sharing information across business functions, enabling timely classification and reporting.

- **Communications with Counterparties and Clients:** We maintain open lines of communication with our counterparties and clients to provide updates and ensure they are informed of any developments that may affect them following a significant business disruption.

- **Communication with Regulators and Authorities:** The Group ensures that incidents in which the Business Continuity Plans are activated and impact warrants notice, including ICT-related events, are reported to the relevant regulatory bodies and authorities. This includes having a designated contact person, team, or function responsible for managing such communications, equipped with the necessary authority, resources, and expertise.