THE GOLDMAN SACHS BUSINESS RESILIENCE PROGRAM (INCLUDING DISASTER RECOVERY)

OVERVIEW

Business Resilience is a high priority for the Goldman Sachs Group, its subsidiaries and affiliates (referred to as "Goldman Sachs", "GS" or "the firm" throughout this document). Our goal is to ensure our continued ability to serve our clients and to protect their assets, as well as safeguarding the people and assets of our firm. Our Business Resilience Program ("the program") has been developed to provide reasonable assurance of business continuity in the event that there are disruptions to normal operations. The program continues to evolve, incorporating the concepts of Operational Resilience. Goldman Sachs is committed to maintaining compliance with regulatory expectations in relevant jurisdictions in which we operate to ensure alignment with Operational Resilience requirements and policies.

The firm has established a global, structured approach to ensure business operations preparedness in the event of an operational disruption. We have developed business continuity plans (BCPs) to address operational disruptions of varying scope and scale, including displaced personnel or a significant reduction in our workforce due to illness, injury or death, or disruptions to critical third parties that the firm depends upon. Operational disruptions caused by cyber-security incidents impacting the confidentiality, availability, or integrity of our systems, and the systems of critical third parties, are also in scope. Responses to external disruptions that may not be specific to Goldman Sachs, such as a pandemic, are also contemplated as part of our approach.

Our plans incorporate resilience capabilities that leverage our global resources and infrastructure, including the ability to relocate impacted business operations using designated and tested business recovery solutions. The firm has the ability to enable staff to operate from non-Goldman Sachs premises, including their homes, through the use of secure remote access solutions should an incident occur which requires personnel to be dispersed. During the Covid-19 pandemic, this capability was proven effective for a prolonged period of time, for all our staff. Our resilience capabilities also include the ability to replicate critical data and applications between geographically dispersed data centers. Examples include, 1) If a local weather disruption renders one or more of our BAU facilities inoperable, critical functions can continue to be performed at another, unaffected, Goldman Sachs office. Alternatively, staff are also able to work from home as applicable, and; 2) If a problem occurs in one data center whereby servers in that data center are inaccessible or have shut down, we can carry on processing from another Goldman Sachs data center. These capabilities enable Goldman Sachs to continue operating during an operational event with minimal disruption or loss of data.

While plans are in place to mitigate the effects of disruptions, crises or events are inevitable and will range in type and severity. No plan is failsafe and there may be circumstances where business disruption could result in undesirable outcomes for the firm.

As part of on-going maintenance of our program, we periodically test system and process failover capabilities, and test our staff's ability to operate from designated people recovery sites as well as non-Goldman Sachs premises, including their homes, through secure remote access solutions.

THE BUSINESS RESILIENCE PROGRAM

The firm is committed to ensuring that its Business Resilience Program is comprehensive and up-to-date, particularly as new information, techniques, and technologies become available. We may alter, add to, or eliminate specific aspects of the program as we deem appropriate for the protection of all concerned. We keep our clients and other stakeholders informed of material changes to the program through updates to this document.

We have a dedicated team of professionals responsible for creating and maintaining the program; implementing, managing, and monitoring the firm's preparedness; and training and educating staff. The Business Resilience Program is comprised of six key elements: Crisis Management, Business Continuity Planning, Technology Resilience, Business Recovery Solutions, Assurance, and Process Improvement and Continual Assessment.

1. Crisis Management

Crisis Management encompasses the communication processes and response procedures by which the firm deploys, post an operational disruption, as well as the tools, training, and exercises we use to help prepare the firm and our people for responding to business disruptions. In order to manage an incident efficiently and effectively, the firm has established a multi-pronged, rapid response capability that includes:

- **Formal Crisis Management Centers (CMCs)** in every region of the firm's worldwide operations. The CMCs enable the firm to monitor its environment, execute pre-established crisis management procedures, and coordinate responses.

- **Crisis Responders** identified and trained to support the assessment, escalation, and decision making processes in an operational disruption.

- **Communication plans with local authorities, and regulators (via appropriate teams)** to facilitate information flow and coordination of responses.

- **Communication plans with stakeholders and staff** that may be impacted by a disruption to Goldman Sachs operations.

- **Processes and communication tools** that are periodically tested to notify key stakeholders and first responders quickly at the onset of an operational disruption and throughout.

- **Training for all employees** on crisis response, and resources available for reporting incidents with the potential to impact Goldman Sachs people or facilities.

- **Standard contractual agreements** with our critical third parties that include notification protocols with Goldman Sachs in the event of a disruption at the third party.

The firm's Crisis Management responses are periodically tested. The firm carries out both desktop drills and live exercises that reinforce these arrangements and allow the firm to continuously improve the program and supporting processes. Our framework takes into account the risk profile of particular locations or regions in the design and execution of the drills and exercises including natural disasters, geopolitical events and other environmental or health hazards.

2. Business Continuity Planning

Business Continuity Planning focuses on protecting client assets and assuring that the firm is able to continue business operations in the event of an operational disruption.

Central to the firm's business recovery efforts is a requirement that each Goldman Sachs business unit develop, test, and maintain plans that document their recovery requirements for its functions. Each business unit identifies its critical activities, the dependent assets (people, facilities, systems, third parties and processes) that support those activities and the impact that a disruption to these dependent assets would have on the business unit's activities. The resultant plans document the recovery strategies and capabilities as well as functional requirements needed to re-establish essential business operations while accounting for any applicable regulatory restrictions (e.g., recovery teams, business recovery solutions, equipment requirements).

3. Technology Resilience

Technology Resilience focuses on the restoration of the firm's core infrastructure, including networking, applications, market-data feeds, and other shared technologies to ensure the continuation of critical business systems processing. Applications must be classified depending on the criticality of the business operations they support and their Recovery Time Objective (RTO - which is the maximum tolerable length of time that an application can be unavailable after an incident occurs) must be defined to document their recovery expectations and a Recovery Point Objective (RPO - which is the maximum tolerable data loss that can be sustained by an application in case of an incident resulting in data destruction or corruption) that minimizes data loss. Applications are then prioritized based on their classification which drives the frequency of application testing.

Wherever practicable, Goldman Sachs physically separates the people conducting business from the technology infrastructure supporting the business, locating them in separate buildings in order to reduce the likelihood of simultaneous personnel and systems disruptions. Additionally, critical systems are deployed across two or more physically distant data centers, or external cloud locations, to support recovery of systems and data in case of a facility disruption. Critical data is also backed up to alternate locations on a regular basis.

In addition, Goldman Sachs' buildings are assessed and aligned based on the requirements of the businesses and technology that are located within them. Resilience capabilities such as protection with Uninterruptable Power Supply (UPS), diversity of utility services and telecommunications, and allocation of backup generators, are all assessed and implemented where necessary to meet the resilience requirements of the business.

4. Business Recovery Solutions

Business recovery solutions focus on ensuring that our business operations can quickly resume when the primary workplace hosting those operations becomes inoperable or is inaccessible. There are three primary capabilities that Goldman Sachs has in place:

- **People Recovery Sites** are redundant work environments that have been established (both near and far sites) for critical business units. These sites, available in all regions, are outfitted with the equipment and functional capabilities for staff to relocate to if required in order to carry on business operations in emergency situations. The sites are continually maintained to ensure operational readiness and are tested regularly.

- **Functional Transfer** arrangements for critical functions are in place as a further safeguard, depending on the type and extent of the operational disruption, and subject to any local regulatory restrictions, allowing those critical functions to be performed by personnel in other principal Goldman Sachs offices.

- **Remote Working Environment** capabilities have been developed so that the firm is able to continue its business by enabling staff to work from their homes or from other non-Goldman Sachs

premises through secure remote access connections.

5. Assurance

Assurance focuses on the regular verification of the effectiveness of our business continuity preparedness, including testing of our technology resilience and business recovery solutions required to demonstrate the ability to meet business recovery requirements during an operational disruption event:

- **Technology resilience** assurance is gained through failover tests, and equivalent means (such as demonstration of live-live processing), based on their criticality to the businesses that depend on them, to ensure the resilience of applications and infrastructure meets the documented requirements.
- **Business recovery solutions** assurance is gained through regular testing of each solution (depending on the criticality of the business function) by:

    1. Ensuring critical functions can be performed from the People Recovery Sites

    2. Confirming the ability to support business operations through Functional Transfer of critical functions to staff in other locations

    3. Ensuring critical staff can effectively perform their functions from recovery sites and/or non-Goldman Sachs premises, such as their home, through testing their remote working environment

Compliance with Assurance requirements is tracked and significant issues escalated to management. As of the date of this statement, Assurance requirements for the last fiscal year including testing of Technology Resilience as well as Business Recovery Solutions have been conducted with no significant issues outstanding.

For critical third parties that the firm depends upon, resilience assessments are conducted on the third parties' business continuity practices. Issues identified are tracked, managed and escalated to management as appropriate.

6. Process Improvement and Continual Assessment

The Business Resilience Program is subject to process improvement and continual assessment of our state of readiness for potential operational disruptions resulting from internal and external events. This includes:

- Consideration of any significant issues or gaps identified during testing activities

- Assessment of risks due to the changing environment and their potential impact to the firm's resilience posture

- Identification of changes to Goldman Sachs' business operations that may affect Business Resilience requirements

- Introduction of new strategies and technologies that become available

- Changes required following regulatory developments, impacting local practices or the global program

The results of these assessments enable us to identify and integrate new risk scenarios into the program as well as drive improvements to our technology resilience and business recovery solutions when needed.

CLIENT COMMUNICATIONS AND QUESTIONS

This document provides an overview of the firm's Business Resilience Program. If you have additional questions, please contact your Goldman Sachs representative. Please bear in mind that we will not respond to specific questions about the program that could compromise our security.

Pertinent updates to this document will be available on the Goldman Sachs website at http://www.goldmansachs.com/disclosures/business-resilience.pdf

This document can also be obtained via mail by contacting your Goldman Sachs representative.

IN THE EVENT OF AN OPERATIONAL DISRUPTION

Should there be a significant operational disruption, clients are encouraged to visit the Goldman Sachs website (http://www.gs.com) for additional information.

Last Certified: March 7th, 2022