Global Operational Resilience Program

THE GOLDMAN SACHS OPERATIONAL RESILIENCE AND BUSINESS CONTINUITY PROGRAM (INCLUDING DISASTER RECOVERY)

Goldman Sachs' Operational Resilience Framework is designed to prevent, respond to, recover from, and adapt to significant operational disruptions that could impact our clients, the market and the firm. Operational Resilience is a high priority for the Goldman Sachs Group and its subsidiaries (referred to as "Goldman Sachs", "GS" or "the firm" throughout this document). Our goal is to provide reasonable assurance of continued ability to serve our clients and to protect their assets, as well as safeguarding the people and assets of the firm.

Fundamental to the delivery of the Operational Resilience Framework are the firm's Business Continuity, Disaster Recovery and Crisis Management programs. Underpinning the delivery of these components are the firm's asset-based resilience programs, encompassing technology disaster recovery, third-party vendor resilience, facility resilience and people wellness.

Resilience Planning

The firm conducts resilience planning through business continuity planning and asset-based resilience programs.

- **Business Continuity Planning** is a global, structured approach designed to govern the firm's preparedness and contingency planning. Business Continuity Plans (BCPs) are developed for the firm's business unit activities and contain details such as criticality of the activities and Recovery Time Objectives (RTOs). Dependent assets, functional requirement and appropriate business recovery strategies including workarounds are also documented. BCPs are reviewed and updated regularly.

- **Asset-based Resilience Programs** focus on obtaining assurance as to the resilience capabilities of the firm's dependent assets. Specifically:

    - **Technology disaster recovery program:** Disaster recovery planning focuses on the firm's planning and testing capabilities to ensure restoration of the firm's core technology infrastructure, including networking, applications, market-data feeds, and other shared technologies to ensure the continuation of critical business systems processing and availability. The firm documents disaster recovery plans to ensure restoration of critical applications and their data after a disruption. Applications have appropriate RTO and Recovery Point Objective (RPO: the maximum acceptable amount of data loss after an unplanned data-loss incident, expressed in time) to define their recovery expectation. The disaster recovery plans detail the procedures required for the recovery of data and applications within their defined RTO and RPO.
    - **Third-party vendor resilience program:** Vendor resilience is evaluated through the firm's Third-Party Operational Resilience Assurance (TORA) and Vendor Business Continuity Planning (VBCP) programs. These programs assess the adequacy and effectiveness of third-party vendor BCP plans and their ability to recover in the event of a disruption. Exit and replacement strategies detailing alternate solutions for a loss of third-party services are also documented for critical vendors of the firm.

- **Facility resilience:** The resilience of Goldman Sachs' buildings is identified via the criticality 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 implemented where necessary to meet the resilience requirements of the business.
- **People wellness program:** The firm supports its employees and families with a broad program of resilience resources. For example, specific proactive monitoring is conducted on potential pandemics from the World Health Organization and Center for Disease Control with a firmwide documented procedure in place to be enacted as necessary.

Crisis Management

Crisis Management encompasses the communication procedures including the tools, training and exercises, required to help prepare the firm and our people for responding to significant business disruptions. To manage an incident efficiently and effectively, the firm has established a multi-pronged, rapid response capability that includes:

- **Formal Crisis Management Centers (CMCs)** across the regions 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 to facilitate information flow and coordination of responses and 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.
- **Third-party protocols** whereby appropriate arrangements are agreed with critical third-parties that include notification protocols with Goldman Sachs in the event of a disruption at the third-party.

Business Continuity and Crisis Response Training

The firm provides training to the personnel involved in the execution and maintenance of business continuity planning across the firm. The training details the roles and responsibilities of key role holders during a business disruption. In addition, training is also provided for employees on crisis response, and resources are available for reporting incidents with the potential to impact Goldman Sachs people or facilities.

Resilience Testing

The firm conducts several testing activities at a set cadence designed to provide the ability to respond, recover and continue business-as-usual:

- **BCP Recovery Strategy testing:** Alternate working solutions such as process handover, homeworking environment and alternate sites are adopted when there is a loss of one or more assets. These alternate methods of working are tested annually as per the standard procedures.
- **Important Business Services (IBS) Integrated testing:** Firmwide IBS (or local regulatory equivalent) have been identified and denote the critical services performed by the firm that if disrupted will cause intolerable harm to clients, the market and/or the firm. Dependent assets integral to the delivery of the

IBS are mapped and are subject to heightened testing requirements to assure their resilience. A combination of physical and tabletop testing, referred to as an Integrated Test, is conducted based on severe but plausible operationally disruptive scenarios to evaluate the firm's IBS' ability to recover their processes.

- **Disaster Recovery testing:** Applications based on their criticality undergo disaster recovery testing at varying cadence to evaluate the application's recovery capabilities.
- **Third-party Vendor Resilience testing:** The firm conducts critical third-party vendor tests to assess the adequacy and effectiveness of a third-party vendor's business continuity plan and their ability to recover within the timeframe required by the business.
- **Crisis Response testing:** The firm's Crisis Management responses are periodically tested. The firm carries out both tabletop drills and live exercises that reinforce these arrangements and allow the firm to continuously improve the program and supporting processes. Our framework includes 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.

As outlined above, resilience testing has been performed as per policy requirements during the previous fiscal year. Compliance of testing requirements is monitored and reported to governance groups as required. Actions resulting from testing are tracked and managed accordingly.

Client Communications and Questions

This document provides an overview of the firm's Operational 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

Last Certified: June 7th, 2024