Global Operational Resilience Program

THE GOLDMAN SACHS OPERATIONAL RESILIENCE, BUSINESS CONTINUITY AND DISASTER RECOVERY STATEMENT

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. The firm's operational resilience posture is reported to the Board regularly to ensure challenge and oversight of the firmwide Operational Resilience program.

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, cyber resilience, third-party vendor resilience, facility resilience and people wellness.

Resilience Planning

The firm conducts resilience planning through management of important business services, business continuity planning and asset-based resilience programs.

- **Firmwide Important Business Services** (or equivalent as required by local regulation) are identified as the critical services performed by the firm that, if disrupted, could cause intolerable harm to clients, the market, or the firm. Impact tolerances (the maximum tolerable level of disruption to an IBS before any significant impact occurs) and dependent assets integral to the delivery of the IBS are identified in planning enabling the firm to establish resilience controls which are necessary for business continuity. The firm's approach to IBS leverages the firmwide business continuity planning program.

- **Business Continuity Planning** is a global, structured program 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 (RTO - Maximum length of time that a BCP can be unavailable after an incident occurs). Dependent assets, functional requirements and scenario agnostic 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. Applications have appropriate Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO - the maximum acceptable amount of data loss after an unplanned data-loss incident, expressed in time), with disaster recovery plans detailing the procedures required to recover data and applications within these defined parameters.

- **Cyber resilience:** The firm prioritizes information security, particularly cybersecurity, to defend against both external threats and internal malicious activities. The firm's Information Security and Cybersecurity Program maintains the confidentiality, integrity, and availability of the firm's information and technology environment. The framework and initiatives of this program are summarized in the Client Security Statement.
- **Third-party vendor resilience program:** The vendor resilience program assesses the adequacy and effectiveness of third-party vendors' ability to recover in the event of a disruption. Exit and replacement strategies detailing alternate solutions for loss of third-party services are also documented for critical vendors of the firm. Where alternate solutions are not readily available, further analysis is undertaken to understand their risk exposure and appropriate remediation is performed such as implementing compensating controls and other resilience enhancement measures.
- **Facility resilience:** The resilience of the firm's facilities is determined by analyzing the criticality of business activities and technology requirements for each location. Resilience capabilities such as 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

The firm's crisis management program employs a coordinated firmwide approach for response and recovery efforts during operational disruptions. To manage an incident efficiently and effectively, the firm maintains 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** with local authorities and regulators to facilitate information flow and coordination of responses, and with external stakeholders and the firm's 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.

Operational Resilience and Crisis Response Training

The firm provides training to the personnel involved in the execution and maintenance of the firmwide Operational Resilience program (including business continuity). In addition, training is provided for employees involved in crisis response to keep them aware of their responsibilities during business disruption. Resources are available for reporting incidents with the potential to impact Goldman Sachs people or facilities.

Resilience and Crisis Management Testing

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

- **BCP recovery strategy testing:** Alternate working solutions such as process handover, homeworking environment alternate sites, and asset workaround strategies are adopted when there is a loss of one or more assets. These alternate strategies are tested annually as per the standard procedures.
- **Important business services (IBS) integrated testing:** A series of simulated response and recovery tests, referred to as IBS Integrated Test, is conducted at least annually based on severe but plausible operationally disruptive scenarios to validate the firm's ability to recover its critical processes.
- **Technology disaster recovery testing:** Applications undergo disaster recovery testing at varying cadences based on their criticality to demonstrate the applications' ability to recover following an operational disruption.
- **Third-party vendor resilience testing:** Vendor resilience is evaluated through the firm's Third-Party Operational Resilience Assurance (TORA) and Vendor Business Continuity Planning (VBCP) programs. As part of these programs, the firm conducts critical third-party vendor assessments to evaluate the adequacy and effectiveness of their business continuity plan and ability to recover within the timeframe required by the business.
- **Crisis response testing:** The firm's crisis management responses are periodically tested through both tabletop drills and live exercises that reinforce expectations during crisis response 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, the firm successfully completed resilience testing 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: 10 June 2025