Morgan Stanley India Primary Dealer Private Limited (MSIPD) Operational Risk - Public Disclosure

Introduction

Risk is an inherent part of our businesses and activities. We believe effective risk management is vital to the success of our business activities. We have policies and procedures in place to identify, measure, monitor, escalate, mitigate and control the principal risks involved in the activities of Morgan Stanley India Primary Dealer Private Limited (MSIPD's) business as well as at the Parent Company level. The principal risks involved in our business activities are both financial and non-financial and is overseen by the Board.

Operational Risk

Operational risk refers to the risk of loss, or of damage to our reputation, resulting from inadequate or failed processes or systems, from human factors or from external events (*e.g.*,cyber-attacks or third-party vulnerabilities) that may manifest as, for example, loss of information, business disruption, theft and fraud, legal and compliance risks, or damage to physical assets. We are subject to operational risks, including a failure, breach or other disruption of our operations or security systems , as well as human error , which could adversely affect our business or reputation. In addition, the interconnectivity of multiple financial institutions with central agents, exchanges and Clearing houses, and the increased importance of these entities, increases the risk that an operational failure at one institution or entity may cause an industry-wide operational failure that could materially impact our ability to conduct business.

There can be no assurance that our business contingency and security response plans fully mitigate all potential risks to us. Our ability to conduct business may be adversely affected by a disruption in the infrastructure that supports our businesses and the communities where we are located. This may include a disruption involving physical site access; software flaws and vulnerabilities; cybersecurity incidents; terrorist activities; political unrest; disease pandemics; catastrophic events; climate-related incidents and natural disasters, electrical outages; environmental hazards; computer servers; communication platforms or other services we use; and our employees or third-parties with whom we conduct business

Culture, Values and Conduct of Employees

Employees of the MSIPD and it group companies / inter affiliates are accountable for conducting themselves in accordance with our core values: *Put Clients First, Do the Right Thing, Lead with Exceptional Ideas, Commit to Diversity and Inclusion,* and *Give Back*. We are committed to reinforcing and confirming adherence to our core values through our governance framework, tone from the top, management oversight, risk management and controls, and three lines of defense structure (business risk, control functions such as Risk Management and Compliance, and Internal Audit).

Risk Management Process

We have established an operational risk framework to identify, measure, monitor and control risk across the MSIPD. Effective operational risk management is essential to reducing the impact of operational risk incidents and mitigating legal, regulatory and reputational risks. The framework is continually evolving to account for changes in the MSIPD and to respond to the changing regulatory and business environment.

In addition, we employ a variety of risk processes and mitigants to manage our operational risk exposures. These include a governance framework, a comprehensive risk management program and insurance

Primary responsibility for the management of operational risk is with the business segments, the control groups and the business managers therein. The business managers maintain processes and controls designed to identify, assess, manage, mitigate and report operational risk. We have a comprehensive Risk Governance Structure within MSIPD and across Morgan Stanley group. Oversight of operational risk is provided by the MSIPD Board and Risk Management Committee, O, regional risk committees and senior management.

The Operational Risk Department ("ORD") provides independent oversight of operational risk and assesses, measures and monitors operational risk.

The Internal Audit Department ("IAD") independently assesses the MSIPD's risk management processes and control. IAD undertakes these responsibilities through periodic reviews of our business activities, operations and systems.

Cybersecurity

Our cybersecurity and information security policies, procedures and technologies are designed to protect our own, our client and our employee data against unauthorized disclosure, modification or misuse and are also designed to address regulatory requirements. These policies and procedures cover a broad range of areas, including: identification of internal and external threats, access control,
data security, protective controls, detection of malicious or unauthorized activity, incident response and recovery planning.

Firm Resilience

The Firm's critical processes and businesses could be disrupted by events including cyber attacks, failure or loss of access to technology and/or associated data, military conflicts, acts of terror, natural disasters, severe weather events and infectious disease. The Firm maintains a resilience program designed to provide for operational resilience and enable it to respond to and recover critical processes and supporting assets in the event of a disruption impacting our people, technology, facilities and third parties.

Third-Party Risk Management

In connection with our ongoing operations, we do not engage into outsourcing of our core functions to external third parties, however, we utilize the services of third-party suppliers, and support from our inter-affiliate groups entities, which we anticipate will continue and may increase in the future. The third party program includes appropriate governance, policies, procedures and enabling technology