BANCO SANTANDER S.A., HONG KONG BRANCH

Operational Risk Disclosure

1.1 Introduction

In accordance with the Basel framework, Santander defines operational risk as the risk of loss due to inadequate or failed internal processes, people, and systems or to external events. It covers risk types such as fraud, technological risk, cyber risk, legal risk and conduct risk.

Operational risk is inherent in all products, activities, processes, and systems, and is generated in all business and support areas.

All employees are responsible for managing and controlling the operational risks generated by their activities.

Our operational risk management and control model is based on a continuous process of identifying, evaluating and mitigating sources of risk, regardless of whether they have materialized or not, promoting that risk management priorities are established appropriately, and internal controls are defined and executed to manage and mitigate the risk across the organization.

1.2 Operational risk management

Management and control model

Our operational risk model establishes the items needed to manage and control operational risk properly according to advanced regulatory standards and best management practices. Its phases are:

• strategic planning;

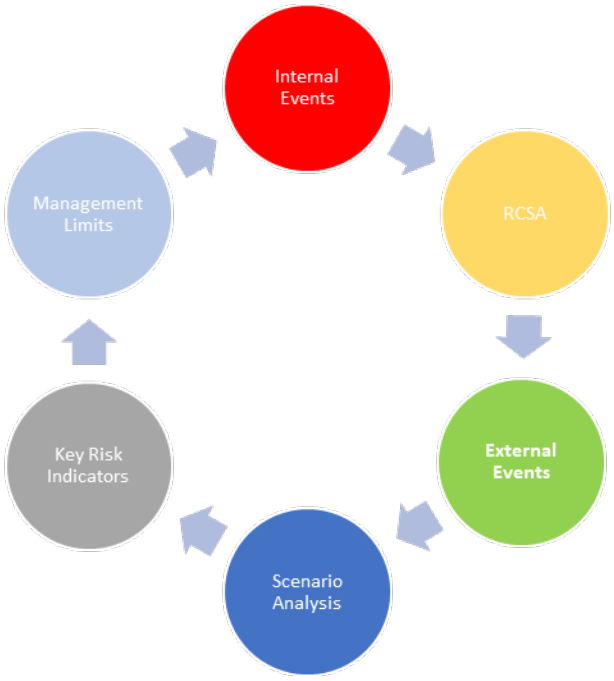
• identification and assessment of risks and internal controls;

• ongoing monitoring of the operational risk profile;

• implementation of actions to manage the risks, including mitigation measures, and

• disclosure, reporting, and escalation of relevant matters.

The main operational risk tools used by the Group throughout the management cycle are the following:



Internal event database: registry of operational risk events, whose impact could be financial (e.g., losses, irrespective of their amount) or non-financial (i.e., relating to regulation, customers, or services). This information inform us of the impact of our operational risk:

- enables the analysis of root causes;
- increases the awareness of risks for better operational risk management;
- enables the escalation of relevant operational risk events to senior risk executives in the shortest time possible;
- facilitates regulatory reporting.

Operational risk control self-assessment (RCSA): a qualitative process that evaluates each area´s operational risks and assesses the control environment based on the opinion of experts from each function. Its purpose is to identify, assess and measure material operational risks that could prevent the business or support units from achieving their objectives. After assessing risks and internal controls, mitigating measures for risk levels above tolerance are identified.

Our RCSA integrates specific reviews that allow to identify cyber, technology, fraud, third party supplier and other risk drivers that could lead to operational risk as well as the failure to meet regulations. In addition, the RCSA incorporates reviews related to regulatory compliance, conduct and financial crime risk.

External events data: quantitative and qualitative information about external operational risk events. This information facilitates detailed and structured analysis of relevant events in the industry.

Operational risk scenario analysis: identifies highly unlikely events that could result in significant losses for us and establishes appropriate mitigating measures based on the assessment and opinion of experts from business lines and risk managers.

Key risk indicators: indicators that provide quantitative information about our risk exposure and control environment. The most relevant indicators are those related to the bank´s main risk exposures, and are part of operational risk management limits.

Management Limits: The risk appetite in Banco Santander is defined at Group level by the board of directors and is cascaded down to subsidiaries through the approval of local Risk Appetite Statements(RAS) in each unit, aligned with that of the Group.

Banco Santander S.A. , Hong Kong branch Risk Appetite Statement (aligned with that of the Group) should be cascaded into the Santander Corporate and Investments Banking management limits and in accordance to the policies for the different risk types.

Other instruments are used to analyse and manage operational risk, such as the assessment of new products and services, and initiatives; business continuity plans (BCP); review of the management perimeter; recommendations from internal and external auditors, and supervisors; and the quality assurance process.

1.3 Operational risk Exposure

Banco Santander, S.A. Hong Kong branch did not have any significant operational loss events during the 2022 exercise.

During the 2022 Internal Control assessment and certification, there was no control identified with material weaknesses.