

## 風險管理

### Management of Risks

#### 總覽

本集團業務的主要內在風險包括信貸風險、利率風險、市場風險、流動資金風險、操作風險、信譽風險、法律及合規風險及策略風險。本集團的風險管理目標是在提高股東價值的同時，確保風險控制在可接受的水平之內。

#### 風險管理架構

本銀行董事會對本集團的整體風險管理負最終責任，並負責訂定風險管理的策略性目標及風險管理架構。

為達至本集團風險管理目標，董事會下設風險管理委員會，並有獨立非執行董事擔任成員，負責監察本集團的各類風險及審批高層次風險管理政策。

行政總裁轄下的多個管理委員會及有關部門，根據董事會訂立的風險管理策略，負責制定及定期檢討風險管理政策及監控程序。

風險管理單位負責制定識別、量度、監察及控制信貸風險、市場風險、操作風險、信譽風險、法律及合規風險、利率風險、流動資金風險及策略風險的政策及程序，設定適當的風險限額，持續監察有關風險。

稽核部獨立查核風險管理政策和監控措施是否足夠及有效，以確保本集團依據該等既定政策、程序及限額營運。

獨立性是施行有效風險管理的關鍵。為保證風險管理部及稽核部的獨立性，風險管理部和稽核部份別直接向風險管理委員會及稽核委員會匯報，該兩個委員會均為董事會下設的專責委員會，全部委員由本銀行董事擔任。

#### THE OVERVIEW

The principal types of risk inherent in the Group's businesses are credit risk, interest rate risk, market risk, liquidity risk, operational risk, reputation risk, legal and compliance risk, and strategic risk. The Group's risk management objective is to enhance shareholder value by maintaining risk exposures within acceptable limits.

#### RISK MANAGEMENT STRUCTURE

The Bank's Board of Directors (the "Board") holds the ultimate responsibility for the Group's overall risk management. It determines the risk management strategies and the risk management structure.

To achieve the Group's goals in risk management, the Board sets up the Risk Management Committee, which comprises of independent non-executive directors, to oversee the Group's various types of risks and approve the high-level risk management policies.

According to the risk management strategies established by the Board, risk management policies and controls are devised and reviewed regularly by relevant departments and respective management committees set up by the Chief Executive.

The risk management units develop policies and procedures for identifying, measuring, monitoring and controlling credit risk, market risk, operational risk, reputation risk, legal and compliance risk, interest rate risk, liquidity risk and strategic risk; to set appropriate risk limits; and to continually monitor risks.

The Audit Department conducts independent reviews on the adequacy and effectiveness of risk management policies and controls to ensure that the Group is operating according to the established policies, procedures and limits.

Independence is crucial to effective risk management. To ensure the independence of the Risk Management Department and the Audit Department, they report directly to the Risk Management Committee and the Audit Committee respectively. Both committees are specialised committees set up by the Board and all members are directors of the Bank.

## 風險管理 Management of Risks

### 風險管理架構 (續)

#### (i) 信貸風險管理

信貸風險管理詳情載於財務報表附註4內。

#### (ii) 流動資金風險管理

流動資金風險管理詳情載於財務報表附註4內。

#### (iii) 市場風險管理

市場風險管理詳情載於財務報表附註4內。

#### (iv) 操作風險管理

操作風險是指由不完善或有問題的內部程序、人員、系統，以及外部事件所造成損失的風險。操作風險隱藏於業務操作的各個環節，是集團在日常操作活動中面對的風險。

集團實施操作風險管理「三道防線」體系：所有部門或功能單位為第一道防線，是操作風險管理的第一責任人，通過自我評估與自我提升來履行業務經營過程中自我風險控制職能。操作風險及法規處連同一些與操作風險管理相關的專門職能單位包括人力資源處、業務規劃及流程優化處、事務處、財務管理處、會計處（統稱為「專門職能單位」）為第二道防線，負責評估和監控第一道防線操作風險狀況，對其工作提供指導。獨立於業務單位的操作風險及法規處，負責協助管理層管理本集團的操作風險，包括制定和重檢操作風險管理政策和框架、設計操作風險的管理機制和工具、評估及向管理層和風險管理委員會匯報總體操作風險狀況；專門職能單位對操作風險的一些特定的範疇或與其相關事項，履行第二道防線的牽頭管理責任，除負責本單位操作風險管理外，亦須就指定的操作風險管理範疇向其他單位提供專業意見／培訓並履行集團整體的操作風險牽頭管理。稽核部為第三道防線，對操作風險管理框架的有效性與充足性作獨立評估，需定期稽查集團各部門或功能單位操作風險管理工作的合規性、有效性，並提出整改意見。

### RISK MANAGEMENT STRUCTURE (Cont'd)

#### (i) Credit risk management

Details of management of credit risk are set out in Note 4 to the Financial Statements.

#### (ii) Liquidity risk management

Details of liquidity risk management are set out in Note 4 to the Financial Statements.

#### (iii) Market risk management

Details of market risk management are set out in Note 4 to the Financial Statements.

#### (iv) Operational risk management

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and system, or from external events. The risk is inherent in every aspect of business operations and confronted by the Group in its day-to-day operational activities.

The Group has implemented the "Three Lines of Defence" for its operational risk management. All departments or functional units as the first line of defence are the first parties responsible for operational risk management, and carry out the duties and functions of self risk control in the process of business operation through self assessment and self enhancement. The Operational Risk, Legal and Compliance Division together with certain specialist functional units in relation to operational risk management within the Group, including the Human Resources Division, Business Planning & Optimization Division, Administration Division, Financial Management Division and Accounting Division (collectively known as "specialist functional units"), are the second line of defence. They are responsible for assessing and monitoring the operational risk conditions in the first line of defence, and providing them with guidance. The Operational Risk, Legal and Compliance Division, being independent from the business units, is responsible for assisting the Management in managing the Group's operational risk, including the establishment and review of the operational risk management policy and framework, designing the operational risk management tools and reporting mechanism, and assessing and reporting the overall operational risk position to the Management and Risk Management Committee. Specialist functional units are required to carry out their managerial duties of the second line defence with respect to some specific aspects of operational risk and its related issues. Besides taking charge of operational risk management in their own units, these units are also required to provide other units with professional advice/training in respect of certain operational risk categories and to lead the Group-wide operational risk management. Audit Department is the third line of defence which provides independent assessment to the effectiveness and adequacy of the operational risk management framework and is required to conduct periodic audit of the operational risk management activities of various departments or functional units within the Group regarding their compliance and effectiveness and to put forward recommendations for remedial actions.

## 風險管理

### Management of Risks

#### 風險管理架構 (續)

##### (iv) 操作風險管理 (續)

集團建立了有效的內部控制程序，對所有重大活動訂下政策及監控措施。設置適當的職責分工和授權乃集團緊守的基本原則。集團採用關鍵風險指標、自我評估、操作風險事件匯報及檢查等不同的操作風險管理工具或方法來識別、評估、監察及控制潛在於業務活動及產品內的風險，同時透過購買保險將未能預見的操作風險轉移。對支援緊急或災難事件時的業務運作備有持續業務運作計劃，並維持充足的後備設施及定期進行演練。

##### (v) 信譽風險管理

信譽風險指因與本集團業務經營有關的負面報導（不論是否屬實），可能引致客戶基礎縮小、成本高昂的訴訟或收入減少等風險。信譽風險隱藏於其他風險及各業務運作環節，涉及層面廣泛。

為減低信譽風險，本集團制定並遵循信譽風險管理政策。此政策的目的是當信譽風險事件發生時本集團能夠盡早識別和積極防範。鑒於信譽風險往往是由各種可能令公眾對本集團信任受損的操作及策略失誤所引發，本集團建立關鍵控制自我評估機制，包括相關風險評估工具，以評估各主要風險可能對本集團造成的嚴重影響，包括對本集團信譽的損害程度。

此外，本集團建立完善機制持續監測金融界所發生的信譽風險事件，以有效管理、控制及減低信譽風險事件的潛在負面影響。集團亦借助健全有效機制及時向利益相關者披露信息，由此建立公眾信心及樹立本集團良好公眾形象。

#### RISK MANAGEMENT STRUCTURE (Cont'd)

##### (iv) Operational risk management (Cont'd)

The Group has put in place an effective internal control process which requires the establishment of policies and control procedures for all the key activities. The Group adheres to the fundamental principle of proper segregation of duties and authorisation. The Group adopts various operational risk management tools or methodologies such as key risk indicators, self-assessment, operational risk events reporting and review to identify, assess, monitor and control the risks inherent in business activities and products, as well as purchase of insurance to mitigate unforeseeable operational risks. Business continuity plans are established to support business operations in the event of an emergency or disaster. Adequate backup facilities are maintained and periodic drills are conducted.

##### (v) Reputation risk management

Reputation risk is the risk that negative publicity about the Group's business practices, whether genuine or not, will cause a potential decline in the customer base, or lead to costly litigation or revenue decrease. Reputation risk is inherent in other types of risk and every aspect of business operation and covers a wide spectrum of issues.

In order to mitigate reputation risk, the Group has formulated and duly followed its Reputation Risk Management Policy. The policy aims to prevent and manage reputation risk proactively at an early stage when an incident occurs. Since reputation risk is often caused by various types of operational and strategic issues that negatively impact the trust and perception of the Group, all operational and key risks identified are assessed through the established Key Control Self-Assessment framework, including risk assessment tools, to evaluate the severity of their impact on the Group, including the damage to reputation.

In addition, the Group has put in place a comprehensive framework to continuously monitor reputation risk incidents in the financial industry. This continuous monitoring enables the Group to effectively manage, control and mitigate any potential adverse impact from an incident. The Group also adopts robust disclosure practices to keep our stakeholders informed at all times, which helps build confidence in the Group and establish a strong public image.

## 風險管理 Management of Risks

### 風險管理架構 (續)

#### (vi) 法律及合規風險管理

法律風險指因不可執行合約、訴訟或不利判決而可能使本集團運作或財務狀況出現混亂或負面影響的風險。合規風險指因未有遵守所有適用法例及規則，而可能導致本集團須承受遭法律或監管機構制裁、引致財務損失或信譽損失的風險。法律及合規風險由操作風險及法規處管理。所有法律事務均由操作風險及法規處處理。操作風險及法規處負責管理法律風險。法律合規風險管理政策是集團公司治理架構的組成部份，由董事會屬下的風險管理委員會審批。

#### (vii) 策略風險管理

策略風險指本集團在實施各項策略，包括宏觀戰略與政策，以及為執行戰略與政策而制定各項具體的計劃、方案和制度時，由於在策略制定、實施及調整過程中失當，從而使本集團的盈利、資本、信譽和市場地位受到影響的風險。董事會檢討和審批策略風險管理政策。重點戰略事項均得到管理層與董事會的充分評估與適當的審批。

本集團會因應最新市場情況及發展，定期檢討業務策略。

### RISK MANAGEMENT STRUCTURE (Cont'd)

#### (vi) Legal and compliance risk management

Legal risk is the risk that unenforceable contracts, lawsuits or adverse judgments may disrupt or otherwise negatively affect the operations or financial conditions of the Group. Compliance risk is the risk of legal or regulatory sanctions, financial losses or losses in reputation the Group may suffer as a result of its failure to comply with all applicable laws and regulations. Legal and compliance risks are managed by the Operational Risk, Legal and Compliance Division. All legal matters are handled by the Operational Risk, Legal and Compliance Division. The Operational Risk, Legal and Compliance Division is responsible for legal risk management of the Group. As part of the Group's corporate governance framework, the policy for the management of legal and compliance risk is approved by the Risk Management Committee as delegated by the Board.

#### (vii) Strategic risk management

Strategic risk generally refers to the risks that may cause current or future negative impacts on the earnings, or capital or reputation or market position of the Group because of poor business decisions, improper implementation of strategies and inadequacies in the response to the changing market condition. The Board reviews and approves the strategic risk management policy. Key strategic issues have to be fully evaluated and properly endorsed by the Management and the Board.

The Group regularly reviews its business strategies to cope with the latest market situation and developments.