
1. General Principles

1.1 In order to implement the strategy goal of the Bank of China Luanda Branch (the Branch), optimize risk management system, make risk management more independent, professional, forward-looking and proactive, guarantee the Branch’s healthy and sustainable business development, and create more values, General Rules of Risk Management of the Bank of China Luanda Branch (2018 Edition) (the “General Rules”) is hereby formulated, pursuant to General Principles of Risk Management of Bank of China Limited (2017 Edition), the Principle of Risk Management (Notice, No.07/2016) and relevant regulatory provisions in Angola. The General Principles is the top programmatic document for the Branch’s risk management, and covers the three lines of defense of internal control.

1.2 Risk refers to the uncertainty of expected returns due to the possible losses, and it exists in all banking activities. The major risks that the Branch is confronted with include credit risk, market risk, operational risk, compliance risk, liquidity risk, country risk, counterparty credit risk, credit concentration risk, interest rate risk in the banking book, strategy risk, reputation risk, money laundering risk and IT risk.

2. Risk management objective

2.1 The Branch’s primary risk management objectives are to optimize capital allocation, maximize value for its shareholders, maintain risk within acceptable parameters and satisfy the requirements of the regulatory authorities, its depositors and other interest groups for the Branch’s prudent and stable development.

2.2 Objective of risk management system construction

(I) Comprehensive risk management scope

Risk management shall cover all risk types and all businesses that may bear risk, according to the principle of “substance outweighs form”.

(II) Bank-wide risk management culture

All the business and management personnel shall recognize BOC’s risk management concept, clearly understand its risk appetite and risk management principles, and accept and strictly implement its risk management systems.

(III) Fully covered risk management process

Risk management shall cover the whole business process, and involve such areas as business development, management control and operation guarantee. As a part of the full process, independent internal audit is the key measure for assessment of integrated risk management.

(IV) New risk management measures
The Branch should continuously draw on the international leading risk management technology, concept and practice, and carry out effective risk management methods in line with economic environment and operating status. Effective risk management methods need risk management technology and information system to realize.

(V) Full-amount risk measurement

Full-amount risk measurement requires the Branch to allocate the economic capital to various types of risks, all departments.

3. Basic principles of risk management

3.1 Basic principles of risk management

(I) Comply with legal and regulatory requirement. Strictly comply with related law and regulations and regulatory rules and guidelines in order to ensure the effective practice of risk management.

(II) Achieve an appropriate balance between risk and return. Appropriate balance of risk and return shall be reached through active control of the benefits and loss, each kind of business should gain benefits matching with the risk it bears, and optimize capital allocation.

(III) Be independent and professional: Risk management departments and personnel should be relatively independent and scientifically manage the risks arising from business development with relatively independent views and professional competence.

(IV) Clarify rights and responsibilities. Strict accountability shall be carried out through perfectly established internal control mechanism, and clearly defined responsibilities of each unit within our organization.

(V) Be forward-looking and proactive: Risk management departments and front-line departments should cooperate with each other, study and manage risks in a forward-looking manner, actively identify, select and bear risks, improve management and control measures, and ensure risks are controllable. Fully “know your clients”, “know your business”. In respect of new products and businesses, risk management departments and front-line departments, based on the principle of “substance outweighs form”, should enhance the access risk assessment and whole-process risk monitoring and ensure that the risk is bearable.

(VI) Be flexible and efficient: The Branch should make proper adjustments in risk management in line with the internal and external situation changes, optimize the management process and intensify efficiency improvement, which will vigorously support the healthy development of businesses.

(VII) Be consistent and uniform: The Branch should implement a uniform risk appetite, risk management strategy and policy standard throughout the whole bank,

---

1 Risk management departments of the Branch include Risk Management Department (RMD), Compliance Department (CD), Finance and Operations Department (FOD), General Administration Department (GAD).

2 Front-line departments of the Branch include Banking Department (BD), Corporate Banking Department (CBD)
in order to ensure consistency between the risk management objective and business development objective.

4. Risk appetite

4.1 Risk appetite refers to the aggregation level and types of risk the Bank is willing to assume within its risk capacity to achieve its strategic objectives and business plan, steady operation and sustainable development, in order to satisfy the expectations of stakeholders, depositors, investors and regulatory authorities, etc.

4.2 The Branch seeks to maintain the moderate risk appetite of BOC and a balance between risk and return in a rational, stable and prudent manner.

4.3 The risk appetite indicators primarily include strategic indicators and key risk indicators (KRI) in key risk categories. Strategic indicators primarily include return on equity (ROE), capital adequacy ratio (CAR), risk-adjusted return on capital (RAROC), external credit rating, etc. Key risk indicators (KRI) mainly refer to risk categories, such as credit risk, market risk, operational risk, liquidity risk, money laundering risk, etc. BOC determines the target values of the indicators above according to regulatory requirements and its development situation, by reference to the average indicators of large domestic commercial banks.

5. Risk culture

5.1 Risk culture refers to the unified consensus on the Bank’s risk awareness, risk-taking behavior and risk management concept.

5.2 The Branch is committed to building a bank-wide risk culture, advocating and establishing values of “being committed, responsible, forward-looking and proactive and professional”. The Bank reflects the risk culture requirements in clear risk appetite, risk management strategy and policies.

5.3 The Branch enhances the bottom line awareness, sense of responsibility, compliance awareness and risk awareness of all staff through scientific performance evaluation, incentive mechanism, training and development.

6. Capital measurement and allocation optimization

6.1 The Branch measures regulatory capital requirements in accordance with the relevant capital management provisions of the Angola’s regulator. The regulatory capital requirements are the bottom lines of various requirements for the Branch’s capital adequacy.

6.2 The Branch employs economic capitals for internal management according to the Head Office requirements. Economic capital refers to the amount of capital that is needed to cover and resist the unexpected loss of the asset portfolio under certain degree of confidence in a certain period in the future. Economic capital is directly interrelated with risk.
6.3 The primary objective of economic capital measurement and allocation optimization is to set the target RAROC to restrict and conduct portfolio management of risk assets with a balance between risk and return, in order to improve the Bank’s capital operation efficiency and achieve sustainable growth.

6.4 Economic capital measurement covers various major risks, such as credit risk, market risk and operational risk, etc. Different methods are adopted in measuring different risks, and different risk capitals can be consolidated.

6.5 Economic capital measurement and allocation optimization mainly include capital planning, capital allocation, measurement and monitoring, portfolio management, analysis and reporting, dynamic adjustment and performance assessment.

7. Risk management framework

7.1 The President’s Office of the Branch. The Branch does not set up a Board of Directors, the President’s Office is the top decision-making organ for risk management in the Bank and assumes the responsibility for implementing comprehensive risk management, and is responsible for:

(I) fostering risk culture;

(II) reviewing risk management framework;

(III) reviewing and approving major risk management policies and procedures;

(IV) approving the information disclosure on the comprehensive risk and various important risks;

(V) other duties related to risk management.

The President’s Office of the Branch may authorize its Risk Management and Internal Control Committee to perform responsibilities of coordinating management and decision-making functions, and perform responsibility of supervising overall risk management.

7.2 The Risk Management and Internal Control Committee (RMICC). It assumes the responsibility for executing the risk management framework and the risk appetite, establishing and improving various risk management systems, supervising the implementation of all departments of the Branch, maintaining the overall operation of the internal control system of the Branch.

Special risk management committees under the RMICC also include Asset Disposal Committee, Credit Reviewing Committee and Anti-money Laundering Committee. Each Committee could report directly to the President’s Office according to the RMICC’s authorized.

7.3 Lead Functional departments for risk management

The Branch’s lead functional departments for risk management are responsible for the management of various risks under the President’s Office. It assumes the responsibility for formulating policies and procedures for risk management and monitoring and managing risks. According to the Branch’s organization structure, the lead functional departments for risk management are made up of the Risk
Management Department (RMD), the Compliance Department (CD), the Finance and Operations Department (FOD), and the General Administration Department (GAD). The main division of responsibility of risk management is as follows:

(I) The RMD takes the lead to manage the credit risk, market risk, counterparty credit risk and credit concentration risk;

(II) The CD takes the lead to manage the operational risk, compliance risk and money laundering risk;

(III) The FOD takes the lead to manage strategy risk, liquidity risk and interest rate risk in the banking book;

(IV) The GAD takes the lead to manage reputation risk and IT risk.

7.4 Business departments

As the first line of defense for risk management, business departments of the Branch which include the Banking Department (BD), the Corporate Banking Department (CBD), should assume the direct responsibility of risk management. It should observe and implement risk management policies and systems in business operation, and should assume the primary responsibility for obtaining information, and judging and controlling risks, and communicate with risk management departments on risk management information in time.

Risk management of business departments adopts a risk management task force mode. Business departments should be subject to the management of the Branch’s functional departments for risk management, in order to ensure each operational department can implement the Branch’s risk management policies and procedures.

7.5 Internal audit position

The Branch’s internal audit position is independent of daily management and implementation, is responsible for assisting the President’s Office in assessing the adequacy and effectiveness of risk management, internal control and governance procedures of the Branch, making and implementing the plan of internal audit. Following the dual reporting system, the position should report to both the President’s Office of the Branch and the Audit Department of the Head Office.

8. Risk management policy system

8.1 BOC sets up risk management policy and system suited to its risk management strategy and risk appetite by multilayer management, in order to guide and restrain risk management act.

8.2 The Bank’s risk management policy and system are divided into general principles of risk management, major policies and systems, fundamental policies and systems, and specific policies and systems by nature.

(I) The General Principles of Risk Management is the top programmatic document for risk management.

(II) Major policies and systems refer to those involving corporate governance and risk management system construction that influence the shareholders’ interests.
Major policies and systems include the general risk management policy for various major risk types and consolidated management policy.

(III) Fundamental policies and systems refer to the client and product policies involving the whole bank’s overall business operation and risk control.

(IV) Specific policies and systems refer to those drafted by each department of the Group, each branch or each subsidiary in compliance with the three-tier risk management policies and systems above, including operating rules and implementation rules.

(V) Lower-tier policies and systems should not conflict with higher-level policies and systems.

8.3 The Branch implements the risk management strategy and appetite of the Head Office and adapts to the policies and systems of the Head Office’s risk management unless otherwise specified.

9. Risk management process

9.1 Risk management process of the Branch includes risk identification, measurement, evaluation, monitoring, reporting, control or mitigation.

(I) Risk identification: the Bank identifies various risks arising from operating activities and the specific factors leading to risks. The Bank should keep close watch on the conversion among various types of risks based on identification of existing risks.

(II) Risk measurement: according to the risk measurement model or method for each type of risk which is developed by the Head Office, the Bank should measure the risk level.

(III) Risk evaluation: for each type of risk that should be assessed, the Bank should evaluate various types of risks and overall risk status according to regulatory requirements and its actual assessment contents and methods.

(IV) Risk monitoring: the Bank should set and continuously improve monitoring indicators, employ appropriate monitoring tools and systems to monitor and analyze risk.

(V) Risk reporting: the Bank should regularly report to the President’s Office and the Head Office, and disclose risk information to investors and the general public in compliance with regulatory requirements.

(VI) Risk control or mitigation: the Bank should manage risks by means of decentralization, offsetting, transfer, hedge, compensation and mitigation, based on accurate assessment and measurement of risks. The Bank should take appropriate and effective measures to control the risk status in excess of early warning indicators (limit, KRI threshold value). The Bank should establish relevant management procedures and emergency response mechanism for abnormal conditions.

10. Risk quantification management
10.1 The Branch should conduct quantitative management of major risks according to various measurement models which are established by the Head Office.

10.2 Under the guidance of the Head Office, the Branch should scientifically set scenarios and conduct stress test pursuant to regulatory requirements and internal management needs. Stress test should cover various major risks and major business areas on and off balance sheet, taking into account the changes in macro-economy. The Branch should take appropriate measures to ensure adequate capital and liquidity according to stress test results.

10.3 The Branch should formulate the recovery and resolution plan and the emergency response plan pursuant to regulatory requirements and internal management needs, ensuring that it is capable of responding to and handling emergencies or crises. By formulating the relevant plans in advance, the Branch should be able to take a series of measures to guarantee to continually provide all the key financial services for the stable operation and restore the normal operations when the Bank is under pressure.

11. **Effective risk data aggregation and risk reporting**

11.1 Pursuant to regulatory requirements, the Branch should promote effective risk data aggregation and risk reporting capacity building, comprehensively understand the regulatory rules and regulations relating to effective risk management, timely track changes in the regulatory rules and regulations, and establish corresponding process, policies and system to provide necessary support, so as to ensure that the Bank can adjust its risk data aggregation and risk reporting processes as required by regulators when supervision framework changes.

11.2 Risk data aggregation and risk reporting capabilities should cover all substantive risk exposure, including off-balance sheet risk.

11.3 Departments in relation to quality of risk data and duties thereof are as follows:

(I) Business departments: Owner of risk data, responsible for quality of basic data.

(II) Lead Functional departments for risk management: Owner of risk data, responsible for quality of risk data.

(III) Accountability mechanism of report: All relevant departments shall be liable for authenticity, integrity and timeliness of information provision thereby and information submitted by the departments shall be reviewed and confirmed by General Manager of respective departments.

11.4 Preparation of comprehensive risk report at the Branch.

According to regulation requirements in Angola and BOC’s H.O policy, the Branch will prepare the comprehensive risk report. The responsibility for report preparation shall be assigned to individuals and the head of the risk management department is responsible for examining the report. The report shall be submitted

---

3 The risk report refers to accurate, clear, and complete presentation of the correct risk information for the appropriate users at right time based on risk data.
at least quarterly to the management and the risk and internal control committee, with a copy sent to Risk Management Department, Credit Approval Department, Credit Management Department, and Internal Control and Legal & Compliance Department of Head Office.

11.5 Details of comprehensive risk report at the Branch.

The Branch’s regular report shall at least include:

(I) Overall risk profile and important inspection and handling opinions of regulatory authorities;

(II) Risk performance analysis, such as analysis of changes of key indicators including capital, risk and return;

(III) Profiles of main risks, such as analysis of industry, term, customer and product mixes and analysis of customer rating, risk mitigation, limit management and capital occupation;

(IV) Risk trend analysis, such as analysis of current trend changes and analysis of future risk trends;

(V) Risk solutions and plans, especially analysis of indicators with abnormal changes and a description of measures taken and to be taken; and

(VI) Other contents required by the management of the Branch.

12. Development of risk management teams

12.1 The Branch should implement the risk management concept and responsibility to each post through improvement of risk management organization framework and continuous training, and enhance training of all employees on risk management concepts and methods, in order to ensure every employee has the risk management consciousness, understands risks from business areas and assume corresponding risk management responsibility.

12.2 The Branch should develop risk task forces, and establish the mechanism for cultivation, development and reserve of risk management talent. The Branch should guarantee the staffing for risk management, optimize staff structure, and enhance the professionalism of risk management personnel.

12.3 In the performance evaluation for each department and post, the Branch should set reasonable performance indicators, guide each department to enhance capital constraint and improve risk management.

13. Supplementary principles

13.1 The General Rules shall come into effect from the date of issuance, and shall be interpreted by the Risk Management Department of the Branch.
Attachment I:
The Risk Management Structure of the BOC Luanda Branch

1. Risk Management Structure (Department Level)

2. Risk Management Structure (Committee Level)
President's Office

Risk Management and Internal Control Committee (RMICC)

- Anti-money Laundering Committee
- Credit Reviewing Committee
- Asset Disposal Committee
Attachment II:

Definition of Major Risks

1. Credit risk:
Credit risk is the risk of loss arising from the failure of a borrower or counterparty to repay a loan or otherwise meet a contractual obligation. Credit risk exists in the trading book and banking book, on and off the balance sheet of a bank. Credit risk includes credit concentration risk and residual credit risk.

2. Market risk
Market risk is the risk of loss in the on- and off-balance-sheet businesses of banks as a result of adverse movements in market prices (interest rates, exchange rates, equity prices and commodity prices). Market risk exists in the trading book and the banking book.

3. Operational risk
Operational risk is the risk of loss resulting from inadequate or failed internal processes, staff and IT system, or from external events. It includes legal risk but excludes strategic and reputation risk.

4. Compliance risk
Compliance risk is the risk of legal sanction, regulatory penalty, substantial financial loss and reputation damage arising from a commercial bank’s failing to comply with laws, regulations and rules.

5. Liquidity risk
Liquidity risk is the risk of a commercial bank’s failing to obtain adequate capitals at a reasonable cost, thus causing failure to pay due liabilities, perform other payment obligations and meet the funding needs for normal operations.

6. Country risk
Country risk is the risk incurred to the Bank arising from the inability or refusal by the borrower or debtor in a country or a region to repay the Bank’s debt, losses suffered by the Bank or its commercial presence in such country or region and other losses, due to economic, political and social changes and events in the country or region.

7. Counterparty credit risk
Counterparty credit risk ("CCR") means the risk that the counterparty defaults before the last cash flow under contract is paid and fails to make payment in accordance with the contract.

8. Credit concentration risk
Credit concentration risk is the risk of loss to a bank arising from the default of a single counterparty or a borrower or a group of counterparties and borrowers.
9. Interest rate risk in the banking book

Interest rate risk in the banking book is the risk of loss to the overall income and economic value of banking book caused by the movements in interest rate and maturity structure. It includes the model risks related to the interest rate risk in the banking book.

10. Strategy risk

Strategic risk is the risk of loss arising from a poor strategic business decision of a commercial bank or the changes in the external business environment.

11. Reputation risk

Reputation risk is the risk of negative observation of the group made by stakeholders (including customers, counterparties, investors, regulatory authorities and the public) caused by the group’s operation, management and other behaviors or external events.

12. Money laundering risk

Money laundering risk is the possibility of money laundering occurring in banks, in the process of providing products and services to their customers.

13. IT risk

IT risk is the operational, legal and reputational risks arising from natural and human factors, technological bugs and management vulnerabilities in the IT operation of commercial banks.