OPERATIONAL RISK GOVERNANCE AND MANAGEMENT FRAMEWORK

Chinabank Insurance Brokers Inc.

Introduction

This Operational Framework is aimed to identify, measure, mitigate, report, monitor and govern risks related to the operation of CIBI.

This framework identifies the units performing operational risk management functions and adopts by reference policies of CIBI as controls to the types of risks that arise from CIBI's current and planned activities and, bases for delineate accountability. The policies of the referenced functions as well as those in this framework should be read as a single document.

Where there are inconsistencies, the policies of the function most directly involved in managing the exposure shall govern.

This framework should be read together with the Code of Corporate Governance Manual of CIBI.

Risk Policies

Chinabank Insurance Brokers Inc adopts an operational risk management framework appropriate for its size, complexity of operations, and risk profile.

The framework looks to preserve stakeholder confidence in the sound operations of CIBI.

CIBI must:

- Understand and articulate its operational risk exposures and the adverse events attendant to these exposures;
- Nominate and demonstrate the effectiveness of appropriate controls to reduce the probability or the severity of operational risk events;
- Be capable of detecting emerging risk events or changes to risk profiles
- Respond in a timely and decisive manner to in-progress events and,
- Provide for recovery of normal operations following the occurrence of an operational risk event.

The operational risk management infrastructure should gather enough information on risk profiles and risk events to provide decision makers the appropriate amount of information to drive expression of risk appetite or direct adjustments to risk exposure.

Risk Dictionary

Operational Risk	Operational risk is the risk to current or projected financial condition and resilience arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events.
CIBI	China Bank Insurance Brokers, Inc.
Risk Profile	The willingness and the ability of a risk-taking unit to take on a risk exposure
Risk Exposure	A posture taken that may cause financial condition or resilience to either return positively or negatively
Risk Taking Unit	CIBI as a company or a functional unit inside an operating company that accepts a risk exposure in pursuit of an objective
Risk Event	An adverse occurrence that results in a risk-taking unit incurring unplanned expense
Risk Control	Proactive actions taken prior to an event to reduce the probability a risk event should occur, or the severity of the impact should there be an occurrence
Risk Mitigation	Proactive actions taken to reduce the impact of a risk-event that has already occurred
Insurance	A contract where a third-party agrees to indemnify another for losses incurred from specific contingencies or perils.
Operating Companies	Any going concern entity that is incorporated to separately execute a function that is part of CIBI's Business Source
Business Lines	A portfolio of similar products or services offered by CIBI to a specified target market
Residual Risk	The amount of expected or realized loss that remains after the application of all controls and mitigation.

Risk Surface

Operational Risk is the exposure of current or projected financial condition and resilience arising from inadequate or failed internal processes or systems, inadequate human resource or human errors and misconduct, or to adverse external events.

Its different facets include exposures to:

Personnel

Personnel comprise the human resources company relies on to execute business and corporate operations. Personnel should understand company's mission, risk appetite, core values, policies, and processes. Personnel should be qualified and competent, have clearly defined responsibilities, and be held accountable for their actions. The skills and expertise of management and staff should be commensurate with company's products and services offered to customers. Strategic plans should anticipate and assess human resource needs and develop plans for maintaining staffing commensurate with company's requirements.

The risks related to Personnel include:

- Recruitment, Staffing, and succession
- Training, development, and continuing education
- Productivity, evaluation, compensation, and remuneration
- Human behavior, human error, or human misconduct
- Separation and off-boarding
- Other concerns related to human resources

The Human Resources owns and maintains the framework for managing the risks related to the human resources company relies on to execute business and corporate operations.

Policies and Process

Operating policies and procedures govern the way CIBI conducts business.

Policies are statements of actions that guide decisions and set standards consistent with company's underlying mission, risk appetite, and core values. Policies should: i) control the types of risks that arise from company's current and planned activities and, ii) clearly delineate accountability and be communicated throughout company.

The Board of Directors or a designated board committee approves operating policies. Management is responsible for developing and implementing the policies. Operating units should review policies against their recalibrations of strategic plans to keep these effective.

Processes include procedures, programs, and practices that structure to what the company does in pursuit of its growth and profit objectives. Effective processes are consistent with the underlying policies and define how activities are carried out and help manage risk. They provide for appropriate checks and balances (such as internal controls).

Management establishes processes to implement significant policies through the systems and methods function.

The systems and methods function designs procedures tailored to company's operations, activities, and business strategies and be consistent with company's risk appetite. They must work with the business to establish proper internal controls to ensure the risk profile of operations remains inside the risk appetite of the Board of Directors.

Management is responsible for establishing a system of internal controls that provide for:

- Organizational structure that establishes clear lines of authority and responsibility,
- Frameworks for monitoring adherence to established policies, and
- Processes governing risk limit breaches or regularizing exceptions.

CIBI employs quality control and quality assurance functions to measure performance, make decisions about risk, and assess the effectiveness of processes and personnel. Quality control ensures that company consistently applies standards, complies with laws and regulations, and adheres to policies and

procedures. Quality assurance is designed to verify that established standards and processes are followed and consistently applied.

The operational risk management function is responsible for implementing:

- A risk assessment process to aggregate then articulate the profile of operational exposures
- Assessment by risk takers of the effectiveness of their nominated controls
- Aggregation of risk data through analyzing financial, operational, and regulatory reports
- Collecting and analyzing incident and event information as well as key risk indicators to determine if there are emerging risks or if there are changes to the risk profile and,
- Ensuring articulation of the information to Management and the Board of Directors

The RISK OFFICER owns and maintains the framework for creating effective, integrated processes to implement business and corporate operations as well designing appropriate checks and balances to reduce probability of failure or severity of impact following failure of the process.

Operating Infrastructure

Operating Infrastructure includes the physical and technological facilities required to conduct business. These include:

- Property, Premises and Leasehold Rights that include the locations from which CIBI conducts business operations whether these be owned or rented. The administrative services function manages CIBI's property, premises, and leasehold rights.
- Furniture, Fixtures and Equipment that include all movable items inside CIBI's offices required for the conduct of business. The administrative services function oversees monitoring of group's furniture, fixtures, and equipment.
- Information Technology Infrastructure that includes all assets connected to any of CIBI's networks for purposes of the capture, transfer, processing, or storage of information related to CIBI's operations. PCCI, however, oversees management and monitoring of CIBI's IT infrastructure.

Operating infrastructure risks that require management include the events behind:

- Acquisition or Procurement
- Capacity Planning
- Maintenance
- Damage or impairment
- Obsolescence and Decommissioning

The Administrative Services Function owns and maintains the framework for managing the physical infrastructure of company.

CBC - Properties and Computer Center, Inc (PCCI) as the in-group provider of information technology services aggregates the management and operation of the information technology infrastructure of CIBI. CIBI and PCCI have a Service Level Agreement and an Event Escalation framework to facilitate monitoring of performance, detection/management of in-progress events.

Externalities

External factors are exposures CIBI may have due to forces or elements not directly related to CIBI or outside the perimeter of its operations. These may include exposures to risk events related to:

- Physical Security that results from unauthorized access to facilities, equipment, and resources as well as to protect personnel and property from damage or harm. The Security function covers management and monitoring of these exposures.
- Network Security that results from compromise or penetration of the infrastructure used to connect computers remains safe from unauthorized access or connection. The Information Security function of the Parent Bank implements with the support of the network security function of PCCI, security operations to protect and preserve company's campus and branch networks, its end nodes and its data center from attack.
- Information Security that results from compromise of confidentiality, integrity, or accessibility of data in use, in transit or at rest, either owned by or in the custody of CIBI. The Information Security function of the Parent Bank implements security operations to protect and preserve the confidentiality, integrity and accessibility of information and data assets in use, in transit and at rest.
- Compliance that results from risks that may erode the franchise value of CIBI such as risks of legal or regulatory sanctions, material financial loss or loss of reputation, from failure to comply with laws, rules, related self-regulatory organization standards, and codes of conduct applicable to its activities. The Compliance function covers these exposures.
- Legal issues caused by a defective transaction; a claim (including a defense to a claim or a counterclaim) being made or some other event occurring which may result in a liability or loss; failure to take appropriate measures to protect assets owned or a misunderstanding of, ambiguity in, or reckless indifference to, the way law and regulation apply to the business. The Bank's Legal team and various transaction advisory teams and external counsel provide guidance to CIBI to minimize these exposures.
- Environment and Social Issues arising from negative events caused by an organization with respect to the environment, to society and to corporate governance. CIBI observes a Sustainability plan related to Environment, Social and Governance initiatives of CIBI.
- Reputational Issues that adversely affect company's ability to establish new or maintain existing business relationships or continuously access varied sources of funding. CIBI has identified its stakeholders of concern and the functions inside the company that are engaged with keeping the stakeholders' trust and confidence.

Third-Party Operational Risks

Third -party risks related to operations are exposures of current or projected financial condition and resilience out of reliance on persons outside the perimeter of the operating company to deliver on obligations to customers or to other stakeholders.

Third-party relationships may be in-group when the dependency is on another operating company inside the China Bank Group or out-of-group where the dependency is to an entity that is not part of the China Bank Group.

The use of third parties does not diminish the responsibility of the persons engaging the third-party to ensure that the activity is performed in a safe and sound manner and complies with applicable laws and regulations.

Third-party risk management process follows a continuous life cycle for all relationships and incorporates planning, due diligence, third-party selection, contract negotiation, ongoing monitoring, and termination. The following areas of third-party operational risk exposures are managed as follows:

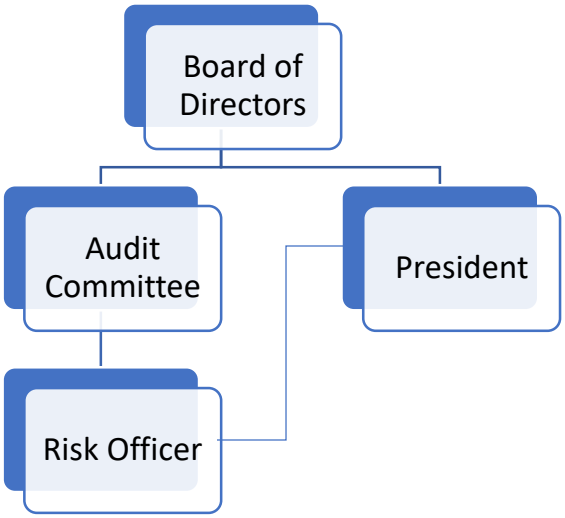
- Inherent Broking Operations – Inherent broking operations are those that the company must perform in-house and cannot rely on the performance of third parties. These include[1]:
    a. Managing Risk Exposures; and
    b. General Management.

- Other Business and Support Operations – Other business operations that qualify for performance by third-parties either on a retainer, an agency, or an outsource basis are managed in consonance with the Outsourcing Framework.

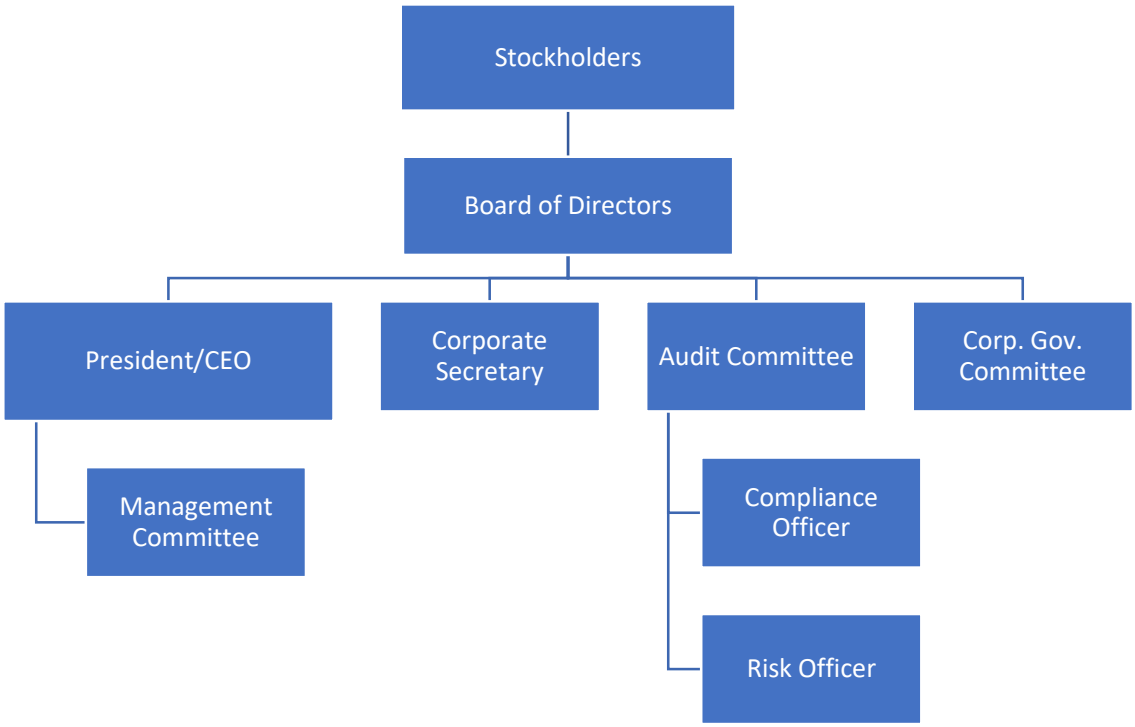
- Information Technology Operations – China Bank's subsidiary, Properties and Computer Center, Inc. (PCCI) is CIBI's Information Technology Operations Service Provider. PCCI aggregates delivery of information technology operations requirements (infrastructure, architecture and solutions) for CIBI and is single point of entry for IT operations services into CIBI.

Operational Risk Management Function

Reporting Line



Organizational Chart



Functional Description

Operational Risk Management

The Risk Officer (RO) is the unit within CIBI that assists the Board of Directors and Management in meeting the responsibility for understanding and managing operational risk exposures and for ensuring the development and consistent implementation of operational risk policies, processes, and procedures throughout CIBI.

Its perimeter covers:

1) Recommend to the board of directors and senior management appropriate policies and procedures relating to operational risk management and controls.
2) Design and implement company's operational risk assessment methodology tools and risk reporting system.
3) Coordinate operational risk management activities across the organization.
4) Consolidate all relevant operational risk information/reports to be elevated/presented to the board and senior management.
5) Provide operational risk management training and advice to business units and on operational risk management issues; and
6) Coordinate with the risk and compliance officers of the parent bank on all CIBI compliance function, internal audit, and external audit on operational risk matters.

Operational Risk Management Process

Dimensioning Risk Profile

CIBI RO is responsible for developing and maintaining an operational risk profile for CIBI.

The operational risk profile should:

1) Map CIBI into operating functions within the group;
2) Identify for each operating unit:
    a. Main business lines, product offerings and channels;
    b. Key personnel and critical processes;
    c. Critical Upstream and Downstream dependencies including critical third-party dependencies;
    d. Key operating assets (tangible infrastructure or intangible data assets);
    e. Key stakeholders and key external exposures.

The operational risk profile shall be the framework against which CIBI shall accumulate Risk and Control Self-Assessments (See Annex – RCSA Template). The Risk and Control Self-Assessment exercise shall be the basis for CIBI to validate the risk profile.

The RO should arrange for presentation of this risk profile to the CIBI Management Committee for acknowledgement and endorsement to the CIBI's Audit/ROC for acceptance.

CIBI RO should maintain the profile and update it periodically following the completion of each Risk and Control Self-Assessment.

CIBI President should arrange for acknowledgement of any changes to the operational risk profile by the CIBI Management Committee and from there endorsement to the CIBI Audit/ROC for acceptance.

RO shall use the acceptance of the Audit/Risk Oversight Committee as basis for documenting the risk appetite for operational risk.

Control Review

The RO is responsible for ensuring each risk-taking unit conducting a Risk and Control Self-Assessments can identify risk exposures taken and nominate controls that reduce either the probability or the severity of a risk event so the residual loss remains inside the appetite of the Board of Directors.

The Risk and Control Self-Assessments (See Annex) should allow the risk taking department to not only nominate controls but to determine their effectiveness.

CIBI Audit/ROC shall challenge the RCSA submissions prior to consolidation when:

- There is a variance between the Audit Report and the RCSA
- There are unfulfilled commitments from the previous RCSA
- There are KRIs related to the value chain analyzed that have turned red for more than three consecutive months in the year prior to the RCSA review.
- There are observed events in LIRS related to the value chain analyzed that reflect either frequency or severity that does not match the rating of the RCSA.

Key Risk Indicators

The Key Risk Indicator Portfolio includes triggers and early warning signs designed to inform Management and the Board of excessive risk-taking.

CIBI Audit/ROC shall identify potential key risk indicators from the RCSA program, the central loss database, other incident and event management databases, internal audit findings and dialogues with management and with functional departments.

(See Annex A-Key Risk Indicators)

Loss Incident and Event Monitoring

The RO manages company's central operational loss database to accumulate a history of operational risk losses that can provide risk data for determining if there are emerging risk events, changes in the effectiveness of risk controls or changes to the operational risk profile.

RO should also require each reporting unit or department to not only narrate the circumstances underlying each event but also to identify the root cause so the operational risk management infrastructure may address the cause and reduce likelihood of recurrence.

(See Annex B – Risk Incidents)

Insurance

RO shall use information it has gathered regarding operation and operating losses to assist the office of the President or Chief Executive Officer in establishing the adequacy of insurance coverage and other insurance needs of CIBI.

The analysis should determine the uninsured, self-insured, or uninsurable operational loss surface of CIBI for purposes of risk acceptance and risk appetite setting.

As insurance is a form of risk mitigation, the division can use information available to it to guide risk taking units in establishing additional controls to minimize or retain risk so exposure remains inside the appetite of the Board of Directors.

RO should investigate risks that carry the potential for catastrophic or significant losses together with the risk taking units to ensure these risks are not retained. Conversely, RO should assist the office of the CEO in identifying losses that are relatively predictable and not severe, therefore not requiring insurance.

RO shall maintain a database of available insurance policies and coverages that should include the:

- covered entities
- coverage provided, detailing major exclusions
- underwriter
- deductible amount
- upper limit and lower limits for claims
- term of the policy
- date premiums are due; and
- premium amount.

RO should also collate records of losses and claims, including whether company was reimbursed. These records indicate where internal controls may need to be improved and are useful in measuring the level of risk exposure in a particular area.

Risk Awareness Training

RO should maintain in cooperation with the Human Resources Group – Training and Development function, an operational risk management module that provides the organization with proper understanding of the operational risk management process.

Operational Risk Governance

Oversight of Senior Management and the Board of Directors

The functions of Senior Management and the Board of Directors in relation to Operational Risk Management, in addition to those appearing on their charters and job descriptions shall be those appearing in this framework.

Responsibility of the Risk-Taking Units

The functions of Risk-Taking Departments/Units in relation to Operational Risk Management, in addition to those appearing on their charters and job descriptions shall be those appearing in this framework

Aggregation of Operational Risk Information

RO shall be responsible for aggregating risk information from all risk taking departments/units of CIBI for purposes of disclosure to the CIBI Audit/Risk Oversight Committee.

RO shall submit reports of risk profiles, risk assessments, control assessments, incident reports and root cause analyses from the functional departments/units upon acknowledgement of the CIBI Management Committee to the CIBI Audit/Risk Oversight Committee.

Risk Management Function

The functions of the Risk Officer in relation to operational risk, in addition to those listed in this annex shall be those outlined in this framework.

Compliance Function

The functions of the Compliance Officer in relation to Operational Risk Management, in addition to those appearing on their charters and job descriptions shall be those appearing in this framework

Governing Regulations

The following regulations govern the management of operational risk in insurance regulated by Insurance Commission.

- IC Circular 2020-71 under the Revised Code of Corporate Governance

All policies contained in this manual should be read as being CIBI's implementation of compliance with the identified governing regulations. Any changes in the narrated regulations that cause inconsistencies with the policies narrated in this manual are deemed adopted pending approval of changes in Board approved documentation.