# Internal Control Framework of RCB Bank Ltd

The internal control departments of the Bank are independent of the business and the units which they monitor and control and they are, also, independent from each other. The purpose, standing and authority of each internal control department is governed by a charter which is approved and periodically reviewed by the Board of Directors of the Bank. Their aim is to ensure that the Bank is operating in full compliance with its banking license and the Regulatory Framework governing the operations of banks in Cyprus. The internal control departments are:

- The Risk Management Department,
- The Compliance Department,
- The Information Security Unit, and
- The Internal Audit Department.

The internal control departments report their findings and assessments to the Board of Directors through the relevant Board of Directors Committees.

## Risk Management Department

The key objective of risk management at RCB is to make sure that all risks are managed in the best possible way for the protection of the interests of all stakeholders. RCB operates through a comprehensive risk management framework to ensure the risks are identified, well understood, accurately measured, controlled and pro-actively managed at all levels of the organisation so that the Bank's financial strength is safeguarded. The risk management department is embedded in all levels of RCB's organisation. The risk management of RCB has adequate system infrastructure, methods and measures to ensure the identification, assessment, control and monitoring of risks and as well as the calculation of the necessary capital to cover the risks assumed.

The Board of Directors exercises its oversight of the Bank's risk management principally through the Risk Committee. The Risk Committee assists the Board of Directors on matters related to risk governance, risk policies and risk appetite setting.

The Risk Management Department (RMD) is an independent department within the Bank. On a quarterly basis, RMD reports on the Bank's risk profile versus its risk appetite to the Board of Directors through the Risk Committee, explaining changes in the risk profile.

The main responsibilities of RMD are the following:

- Assurance that all material risks are identified, measured and properly reported;
- Participation in elaborating the Bank's risk strategy, risk appetite framework and risk limits;
- Independent on-going assessment of risk-bearing activities;
- Responsibilities for the proper planning, development and monitoring of, and reporting on, the risk management framework;
- Examination of all dimensions of the risks the Bank is facing including non-financial risks such as legal and reputational risks;
- Independent assessment of a breach or violation of approved risk limits;
- Participation in the process of approving the development in new markets, products and services and significant changes to existing ones;
- Monitoring Operational Risk by maintaining record for operational loss events and reviewing Key Risk Indicators.

## Compliance Department

The Compliance department aims to promote and sustain a corporate culture of compliance and integrity within RCB and to assist the Board of Directors in developing and implementing an effective compliance framework for the prompt and on – going compliance of the Bank with its legal, regulatory and business obligations.

The Compliance Department (CD) is independent and reports to the Board of Directors through the Audit Committee and to the Chief Executive Officer.

The main responsibilities of CD are the following:

- Compliance of the Bank's activities with the Regulatory Framework and banking business practice; communication to the various units/department/local branches of the Bank the parts of the Regulatory Framework which affect their areas of operations.
- Efficient management of compliance risks, including consolidated analysis of risks, acceptable level of such risks and measures for the timely identification, assessment, control and monitoring of such risks for the purpose of their mitigation;
- Further development of the Banks' governance system;
- Preventing the Bank and the Bank's employees from participating in any unlawful activities, including but not limited to corruption, illegal use of insider information and market manipulation;
- Reinforcing the Bank's reputation and investment appeal on the financial market;
- Ensure compliance with the Prevention and Suppression of Money Laundering Activities Law of 2007 to 2014 and the CBC's directives and circulars for the prevention of money laundering and terrorist financing;
- Ensure compliance of foreign subsidiaries and foreign branches with the corresponding law and regulations in the country or countries in which they are incorporated and in which they operate.
- Ensure that all obligations and reporting of the Bank, its subsidiaries and foreign branches emanating from the Regulatory Framework are carried out within the deadlines allowed;
- Advise and assist the relevant persons responsible for carrying out investment services and activities to comply with the Bank's obligations under the Investment Services and Activities and Regulated Markets Law of 2007 and related directives.
- Advise and respond to queries on compliance issues from the Bank's employees.

### Information Security Unit

The main aim of the information security unit in RCB is to ensure that all components of the Bank's information security program are effective and adequate.

The Information Security unit (IS) reports to the Board of Directors through the Risk Committee.

The IS is a structural unit of the Security Department of the Bank. The main responsibilities of the unit are the following:

- Oversight of the dissemination and implementation of the information security program institution-wide;
- Development and oversight of the implementation of core policies and procedures regarding information security; cooperation with the Bank's business and support departments and other internal control departments for the effective implementation of security principles in the development of their policies and procedures;
- Oversight of procedures designed to prevent unauthorized physical access to the Bank's information assets and participation in the management of physical access rights in the access control system;
- Oversight of appropriate controls for the protection of the Bank's information during termination of employment, long-term absence, transfer or change of duties;
- Participation in the development of measures for credit card and ATM security;
- Active involvement in the development and implementation of an education and training program on information security matters for employees.

### Internal Audit Department

The Internal Audit Department (IAD) is an independent unit that supports the Board of Directors in maintaining efficient and effective Bank operations by monitoring the internal control environment and systems, carrying out audits and providing recommendations for improvement of the Bank's internal control framework. The IAD reports to the Board of Directors through the Audit Committee.

The main responsibilities of IAD are the following:

- Providing independent assurance to the Board of Directors of the Bank in respect of matters such as:
  - Appropriateness, adequacy and effectiveness of the governance framework;
  - Reliability, integrity and completeness of the accounting, financial reporting and management information and information technology systems;
  - Design and operational effectiveness of the Bank's individual controls and internal control departments in respect of the above matters.
- Performing audit assignments in accordance with the annual audit plan and monitoring the implementation of any recommended actions.
- Reporting to the Board of Directors through the Audit Committee, at least on a quarterly basis, all major observations emanating from the audits carried out as well as recommendations for addressing any weaknesses identified.