Board Paper No : 2024/666/04/A

Board Meeting No : 72 Date :2024/04/05

Lanka Credit and Business Finance PLC

Risk-Based Compliance Program / Plan and Compliance Testing Procedure

\

Owner - Compliance Department
Approval – Board of Directors
Date of Approval – 5th April 2024

1. Risk-Based Compliance Program / Plan

The Authority adopts a risk-based approach to compliance, focusing on the risks stemming from non-compliance. It assesses these risks to guide the selection of compliance tools and resource deployment, aiming to minimize risk and maximize compliance.

A risk-based compliance program is a strategic approach that organizations adopt to effectively manage compliance risks. It involves identifying obligations, establishing controls, and promoting continuous improvement.

Here are some key points about it;

1. **Understanding Compliance Risk**:

   Compliance risk refers to the threat an organization faces due to violations of laws, regulations, codes of conduct, or internal standards.

   It can impact an organization's financial stability, reputation, and overall well-being.

2. **Risk Assessment**:

   Company conducts compliance risk assessments to identify and evaluate potential risks. These assessments help understand the full spectrum of compliance risks across different parts of the organization.

   The goal is to allocate resources effectively to mitigate the most critical risks.

3. **Prioritization**

   The highest compliance risks are given priority. These are the risks that could significantly impact an organization's financial, organizational, or reputational standing.

4. **Controls and Procedures**

   Organization then develops controls, policies, and procedures to address these high-priority risks. The goal is to reduce these risks to acceptable levels.

5. **Continuous Improvement**:

   Once the highest risks are mitigated, attention shifts to lower risks. The process is ongoing, with regular assessments and adjustments.

2. Compliance Testing

Compliance testing, also known as compliance audit or regulatory testing, is a crucial process in the financial industry. It involves assessing and evaluating an organization's adherence to relevant laws, regulations, policies, and industry standards.

The primary objective of compliance testing is to identify potential risks, gaps, and weaknesses in a company's compliance program and to ensure ongoing regulatory compliance.

2.1 Compliance Testing Methodology

Risk-Based Approach

A risk-based approach to compliance testing allows organizations to focus their resources on high-risk areas, ensuring efficient and effective testing.

This approach entails identifying, assessing, and prioritizing regulatory requirements based on the potential impact on the organization.

2.2 Implementation of Compliance Testing Programs

- **Identification of Regulatory Requirements:**
  A comprehensive understanding of the relevant regulations, laws, and industry standards is crucial for developing a tailored compliance testing program.

- **Risk Assessment and Prioritization:**
  Assessing the inherent risks associated with each regulatory requirement allows organizations to prioritize their testing efforts on high-risk areas.

- **Test Plan Development:**
  Creating a detailed test plan that outlines the scope, objectives, methodology, and resources required for each test.

- **Execution of Tests:**
  Implementing the test plan, including conducting substantive and control tests and utilizing appropriate sampling techniques.

- **Reporting and Remediation:**
  Documenting the test results, identifying areas of non-compliance, and developing a remediation plan to address any gaps or weaknesses.

2.3 Key Components of Compliance Testing

- **Compliance Policies and Procedures**

  Establishing and maintaining robust compliance policies and procedures that reflect the organization's commitment to regulatory compliance and provide clear employee guidance.

- **Training and Awareness Programs**

  Implementing comprehensive training and awareness programs to ensure employees understand their compliance responsibilities and the consequences of non-compliance.

- **Monitoring and Surveillance**

  Conducting ongoing monitoring and surveillance activities to identify potential compliance breaches and evaluate the compliance program's effectiveness.

- **Internal Controls and Governance**

  Establishing strong internal controls and governance structures to support the organization's compliance efforts and ensure accountability at all levels.

- **Reporting Mechanisms**

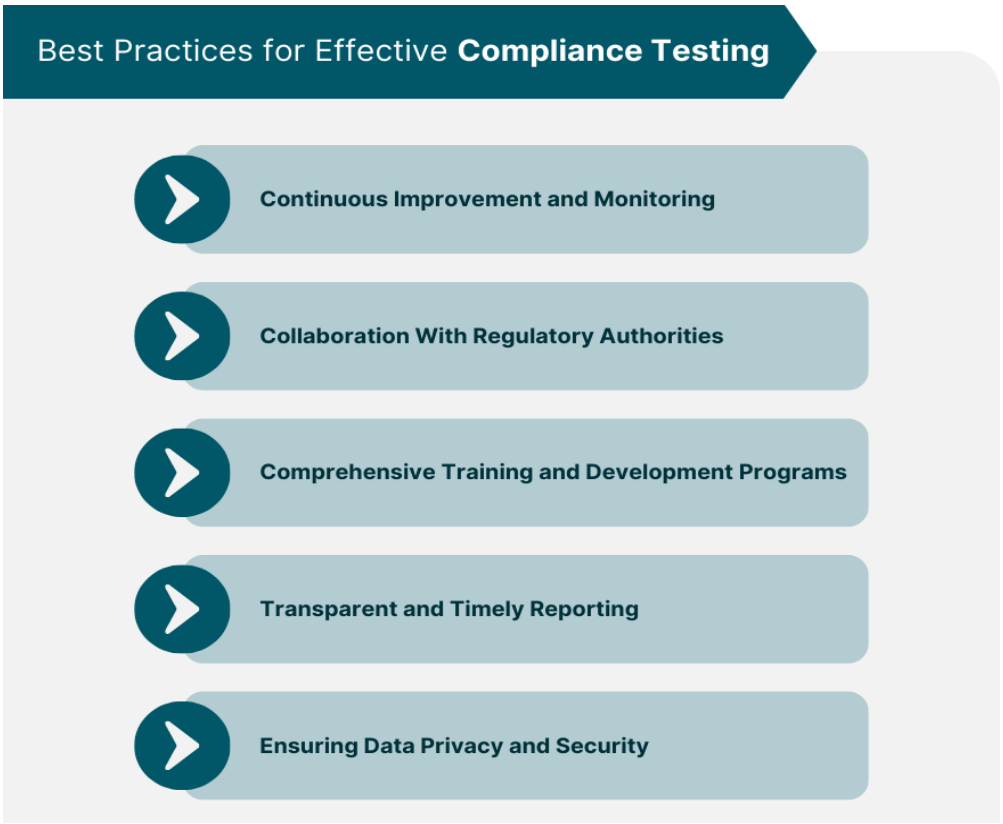
  Developing transparent and timely reporting mechanisms to communicate compliance testing results, findings, and remediation actions to relevant stakeholders, including senior management and regulatory authorities.

2.4 Types of Compliance Tests

- Substantive Testing:
  Assessing the accuracy and completeness of financial transactions and disclosures to ensure compliance with relevant regulations

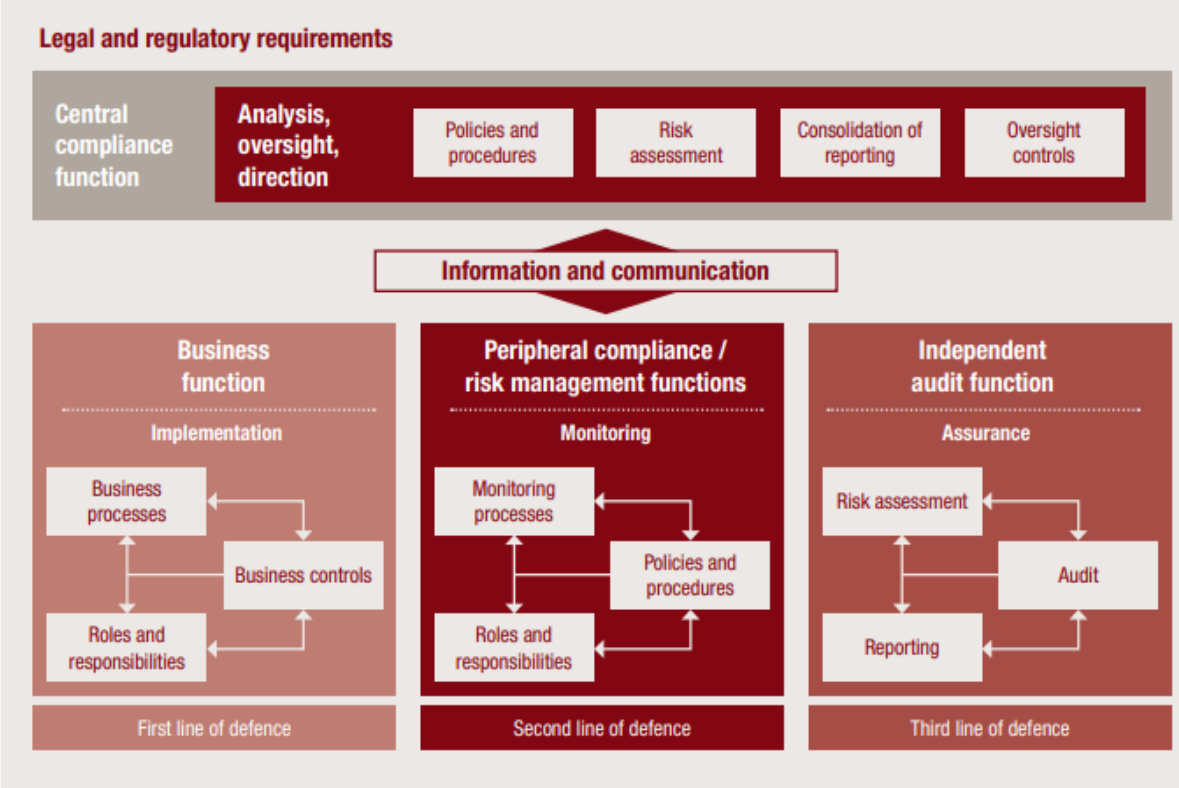
- Control Testing:
  Evaluating the effectiveness of an organization's internal controls, policies, and procedures in ensuring compliance with applicable regulations.

- Random Testing:
  process where regulatory bodies select individuals, firms, or entities for examination without any specific reason or suspicion. Random testing serves as effective policy tools to encourage regulatory compliance. Knowing that anyone could be audited at random encourages adherence to rules and regulations.



3. Aligning compliance testing across the three lines of defense

compliance testing is not always optimally aligned across the three lines of defense. One way to improve the efficiency of testing activities is to align compliance testing across the three lines of defense.



4. ANNUAL COMPLIANCE PLAN – COMPLIANCE DEPARTMENT 2024/2025

Low Risk Medium Risk High Risk

No	Subject	Description	Risk type	Frequency
1.	**Compliance Audit**	A branch compliance audit is a systematic and independent examination of Company's operations, processes, and procedures to determine whether they align with applicable laws, regulations, internal policies, and internal circulars This process helps identify areas of non-compliance, enabling corrective actions to be taken promptly	**Medium Risk** L M H	**Quarterly** – 5 branches **Monthly -** 2 branches (Random ongoing visits)
2.	**Compliance Department Related Policies and procedures**	- Compliance Policy - PEPs Policy - AML/CFT Policy - Risk base procedures manual for KYC/CDD & Risk Categorization - Compliance key Performance Indicators -	**Medium Risk** L M H	To be reviewed by **annually**
		-		
3	**Company's policies/ Manual and procedures**	• All business /administrative related areas polices/procedures,…(other departments related) • Proactively follow up and send reminders in advance regarding due dates of Policies, Manuals & TORs reviews for respective policy owners. • Maintain an updated list of Policies, Manuals & TORs with the details of policy owner, last reviewed date, next review date etc.	**Low Risk** L M H	To be monitored by **annually and ongoing process**

No	Subject	Description	Risk type	Frequency
4	**Branch wise Quarterly Compliance Certificate**	Compliance Certification to be obtained from branches pertaining to AML/CFT policy, PEPs policy, KYC/CDD manual, Compliance manual and internal Circulars.	**Low Risk** **L** / **M** / **H**	**Quarterly**
5	**Department wise Quarterly compliance Certificate**	Compliance Certification to be obtained from departments pertaining to adherence and complied for the related CBSL directions, guidelines, circulars	**Low Risk** **L** / **M** / **H**	**Quarterly**
6	**Central Bank Returns – FINNET Returns**			
6.1	**CBSL Regulatory returns for submission** **Finnet Returns – CBSL**	Ensure timely submission of returns to regulatory authority.	**Medium Risk** **L** / **M** / **H**	**Ongoing Process**
6.2	**Return Verification and data accuracy process**	Regulatory Return Reviews will be conducted based on the criticality of the information submitted to the regulatory authority which includes in the return.	**Medium Risk** **L** / **M** / **H**	**Ongoing Process**
7	**Financial Intelligence Unit – Central bank of Sri Lanka – goAML Global System**			
7.1	**FIU CBSL Reporting AIF(A)/AIF(T)/PAE/RAPS**	In terms of the Section 15 (1) (b) of the Financial Transactions Reporting Act No. 06 of 2006, the Financial Intelligence Unit required to information relating to the persons/ entities /accounts through the goAMl system	**High Risk** **L** / **M** / **H**	**Ongoing reporting**
7.2	**Cash Transaction over 1.0 Mio (CTR)**	In terms of the Section 15 (1) (b) of the Financial Transactions Reporting Act No. 06 of 2006, the Financial Intelligence Unit required to cash transaction (CTR) over 1.0 mio through the goAMl system	**High Risk** **L** / **M** / **H**	**Bi-Monthly**

No	Subject	Description	Risk type	Frequency
7.3	**Gold Loan Transaction / Auction over 1.0 Mio**	In terms of the Section 15 (1) (b) of the Financial Transactions Reporting Act No. 06 of 2006, the Financial Intelligence Unit required to gold transaction/Auctions over 1.0 mio through the goAMl system	**High Risk** L M H	**Bi-Monthly**
7.4	**Electronic Fund Transfers (EFT) over 1.0 Mio**	In terms of the Section 15 (1) (b) of the Financial Transactions Reporting Act No. 06 of 2006, the Financial Intelligence Unit required to Electronic Fund Transfer over 1.0 mio through the goAMl system	**High Risk** L M H	**Bi-Monthly**
7.5	**suspicious transaction reporting (STR)**	Suspicious Transaction Report (STR) is one of the most important report types which is used by the FIU, for its intelligence management processes. Initially, Reporting Institutions (RIs) submitted STRs to the FIU via goAML system	**High Risk** L M H	**Ongoing reporting**
7.6	**Customer inquiries – FIU/NDNBFI**	The Financial Intelligence Unit shall collect or require the supervisory authority of a financial institution to collect any information that the Financial Intelligence Unit considers relevant to an act constituting an unlawful activity, or an offence of money laundering or financing of terrorism, or a terrorist activity whether or not publicly available, including commercially available databases, or information that is collected or maintained, including information that is stored, in databases maintained by the Government	**High Risk** L M H	**Ongoing reporting**
8	**Anti Money Laundering (AML)/ Prevention of Terrorist Financing Related procedures**			
8.1	**Customers Risk profile updating**	Company is required to perform Risk Based Compliance and Risk profiling of all customers is mandatory and is to be done by way of the information derived by the Company through the KYC and Customer Due Diligence (CDD) process	**Medium Risk** L M H	**Ongoing**

No	Subject	Description	Risk type	Frequency
8.2	**Customer screening**	Ongoing monitoring of Customers transaction (through core system) to identify/ track suspicious transactions and transaction trends to ascertain whether transactions are consistent and in line with the customers' known profile. Respective staff members are required to be well acquainted with the system.	**High Risk** L M H	**Ongoing Process**
8.3	**Sanction List Screening**	The company must verify whether any prospective customer or beneficiary appears on any suspected terrorist list or alert list issued in compliance with the United Nations Regulations No. 1 of 2012 published in Gazette Extraordinary No. 1758/19 dated May 15, 2012 and United Nations Regulations No. 2 of 2012 published in Gazette Extraordinary No. 1760/40 dated May 31, 2012, relating to the prevention and suppression of terrorism and terrorist financing, inclusive of United Nations Security Council Resolutions 1267 and 1373	**High Risk** L M H	**Ongoing Process**
8.4	**Identifying and monitoring of High-Risk Customers**	The enhanced CDD measures to business relationships and transactions to customers high risk customers	**High Risk** L M H	**Ongoing reporting**
8.5	**KYC /CDD ongoing monitoring and updating**	Company is required to implement and ongoing monitoring a Customer Due Diligence programme (CDD) and KYC requirement	**High Risk** L M H	**Ongoing reporting**

No	Subject	Description	Risk type	Frequency
9	**Training and Awareness programs**			
9.1	AML / KYC training and other Regulatory aspects	1. Ensure that operational staff maintains an awareness of AML/KYC policies, procedures in order to deliver the daily business requirements 2. With the assistance of HRD, review of existing e-learning module for AML training conducted for existing staff 3. Conducting trainings for new recruits /familiarizations programs	**Medium Risk** L M H	**Ongoing**
10	**CBSL New Directions/ Guidelines/ Circulars...**			
	Compliance with new Directive of CBSL	• Circulate to Board of Directors when request • Circulate to through circulars as appropriate • Prepare a Gap analysis • Implementation of the requirements in the direction • Prepare and obtain board approval for manuals where applicable • Follow up of the implementation	**Low Risk** L M H	**Ongoing**
11	**Other activities**			
11.1	**New products services and systems**	Assistance in aligning new products, services and systems to be within rules and regulations as specified by the regulator. (review will be based on the Advertising rules for NBFI sector regulations issued by CBSL)	**Medium Risk** L M H	**Ongoing**
11.2	**Advice pertaining to the Laws and Regulations issued by the Regulators**	Acting in an advisory capacity on the Laws and Regulations issued by the Regulators in order to assist the staff in operational activities.	**Medium Risk** L M H	**Ongoing**

No	Subject	Description	Risk type	Frequency
11.3	Financial Ombudsman	Processing of customer complaints received through the various reporting mechanisms by coordinating with the business lines. Represent Bank at Financial Ombudsman inquiries over customer disputes.	**Low Risk** **L** | **M** | **H**	**Ongoing**
11.4	Association of Compliance Officers of Finance House	Represent and actively participate for Finance House meetings / webinars and share knowledge and experiences and infuse and share that knowledge with the employees of the company.	**Low Risk** **L** | **M** | **H**	**Ongoing**
11.5	SLIPS	Check the respective regulations and in the event of any non-compliance, take measures to rectify the same with immediate effect.	**Low Risk** **L** | **M** | **H**	**Ongoing**

5. REVIEW OF POLICY

Both Sections of this document should be reviewed annually or as and when the need arises to incorporate new developments and changes and approval should be obtained from the Board of Directors of the company, through BIRMC by the Compliance Department

6. RECOMMENDATION

Recommended to the Board of Directors for adoption

HEAD OF COMPLIANCE