COMMERCIAL CREDIT AND FINANCE PLC

Risk Management and Internal Control Policy
(Risk Management Framework)

TABLE OF CONTENTS

1. Version Control

This policy will be reviewed once in every financial year or in the event of any changes in the regulatory requirements. The updates will be recorded in the "Version Control" with details of revisions and effective dates.

Version Code	Activity	Board Approved Date	Process Owner
1	Implementation	30th November 2020	Chief Risk Officer
2	Review	31st January 2024	Chief Risk Officer

2. Introduction

The Risk Management involves identifying, assessing, avoiding or reducing the negative impacts arising from current or future hazards. The ability to manage multiple risk factors arising across multiple locations, product categories, asset classes, customer segments and functional departments is one of the key factors that determines the degree of success and sustainability of the company. The risk management capabilities facilitate a robust and risk based decision making processes to ensure that the Company continues to create value to its stakeholders.

3. Responsibility

The Board of Directors are responsible to ensure that the risks are appropriately managed within the Company and the Corporate Management take proactive measures to instill the principles of responsible risk management among employees at all levels. The Board delegates the over-sighting of overall risk management of the company to the Board Integrated Risk Management Committee.

4. Objectives of the Risk Management Framework

The company should maintain a robust risk management framework to ensure that the risk management at the company forms a basis to achieve the goals and objectives of the company.

1. Business decisions should be made in a manner that the safeguard of stakeholders' interest.
2. Underlying systems and processes permit the creation of risk awareness across the entire Company and identify measure, analyze, evaluate treatment and monitoring risks.
3. Set risk appetite in order to manage such identified risks.
4. The Shared Values of the Company form a very fundamental aspect of the Risk Management.

5. Risk Management Architecture

The architecture of the risk management includes an independent Risk Management Department, Board-approved risk appetite and risk tolerance levels along with well-defined procedures to support effective management of risk.

The following senior management level committees have been established by the Board Integrated Risk Management Committee of the Company to assist the risks management function.

- Assets and Liability Management Committee (ALCO)
- Executive Credit Committee (ECC)
- Information Security Steering Committee (ISSC)
- Information Technology Steering Committee (ITSC)

The Risk Management Team (RMT) monitors all key risks in line with Board approved risk appetite limits and plays a key role in assisting the Board in its routine risk reviewing process. The RMT should perform periodic assessments to determine any shift in the risk profiles based or new developments or trends in the macroeconomic environment. Need-based assessments should be carried out in times of uncertainties. The RMT is also tasked with monitoring new and emerging risks within the Company's risk universe.

Business decisions should be made in a manner that the safeguarding of stakeholders' interest of the Company from various sources of risk while achieving the company's strategic objectives. Underlying systems and processes should create a risk awareness across the entire Company by identify, measure, analyze and evaluate risks. Processes should be in place to develop and implement appropriate response according to the set risk appetite in order to manage such identified risks. As in the case of all activities of the Company, the Shared Values of the Company should form a fundamental aspect of Risk Management at the company.

The activities of the company's Risk Management system take place at three broad levels as follows:

5.1 Strategic Level

At the strategic level, Risk Management functions should be performed by the Board of Directors and the Board Integrated Risk Management Committee (BIRMC). Tasks include defining risks, ascertaining risk appetite, formulating strategies and policies for managing risks and establishing adequate systems and controls to ensure that overall risk remains within the risk appetite.

5.2 Management Level

At the management level, Risk Management within business areas or across business lines ensures that strategies, policies and directives approved at the strategic level should be operationalized. Development and implementation of underlying procedures, processes and controls should be ensured at the management level. Assuring the compliance with laid down

policies, procedures and controls, and reviewing the outcome of operations, and measuring and analyzing risk related information should be performed at this level.

5.3 Operational Level

The operational risk management is cascaded down to the operational level via the three-lines-of-defense mechanism that reflects the Company's policy that "managing risk is everyone's responsibility". At the operational level, Risk Management activities should be performed by individuals who take risks on Company's behalf, which includes front, middle and back office personnel. They should comply with the approved policies, procedures and controls. Operational level personnel give valuable inputs to continuously improvement of the risk related activities undertaken in the operations. The risk management should establish a methodology to obtain such inputs.

As such all business heads and location heads are deemed the first-line-of-defense and are held accountable for identifying and managing risk and operating within the approved risk policies. The second-line-of defense comprises the Risk Management Team (RMT) and the Compliance Team (CT) headed by independent CRO and CO respectively. Due diligence procedures conducted by the Company's internal audit team and external auditors act as the third-line-of-defense in

providing independent assurance regarding the overall efficacy of the Company's Integrated risk management framework in meeting its stated objectives.

6. Risk Management Process

A comprehensive Risk Management process, which involves identify, analyze and control and review according to the guideline laid out in Annexure 1. The process should be continuously reviewed by the Board Integrated Risk Management Committee (BIRMC) together with the Operations Management Teams. The Management Level sub-committees should meet regularly and are responsible for identifying and analyzing risks. The identified risks should be taken up for discussion at risk sub-committee meetings. The minutes of the sub-committee meetings should submitted to the BIRMC as per the TOR of the subcommittees. The BIRMC should inform the board any significant risk matter through the risk note. The decisions and directives of the BIRMC need to be effectively communicated to the Operational Management through sub-committees for operationalization of such decisions and directives. The BIRMC meets on a regular basis to review and discuss various reports related to Risk Management presented to the Committee by the Management and the findings of the risk sub-committees.

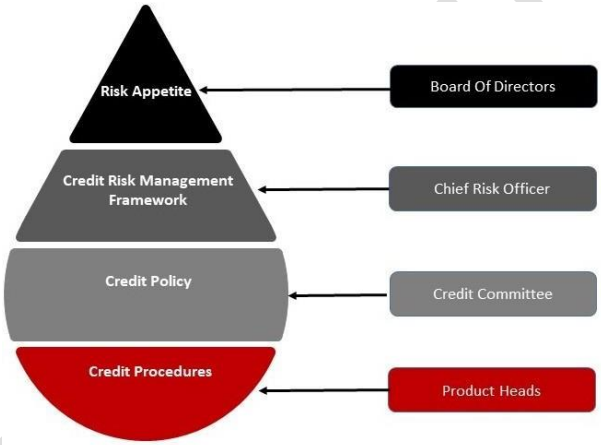
7. Types of Risks

In pursuing the Company's desired strategic objectives, the company is exposed to several risks which have been categorized as follows.

7.1 Credit Risk

Credit risk is the risk of financial loss if a customer or counter party fails to meet a payment obligation under a contract. The Company's credit risk arises mainly from various accommodations granted and can be identified as the most significant risk faced by the Company. The credit risk management objective is to minimize credit risk while ensuring optimal risk rewards pay off for the finance institution, maximize the return, and maintain the quality of the portfolio by minimizing the non-performing loans and probable losses. The credit risk is managed through the credit risk management framework of the company.

- **Credit Risk Management Structure and Approach**



The executive credit committee should implement plans and decisions in order to effective management of credit risk.

The following policies play a central role in managing credit risk of the company

- Credit Risk Management Framework
- Credit Policy and Product Procedure
- Recovery policy
- New products development Policy
- Stress Product Management Policy
- Recognition and Measurement of Financial Instruments Policy

7.2 Market Risk

Market risk is the risk arising from fluctuations in market variables such as interest rates, foreign currencies, equity prices and commodity prices. This is the risk that the fair value or future cash flows of financial instruments will fluctuate due to changes in the market variables. As the Company's operations involve granting accommodations, accepting deposits and obtaining funding facilities, the movements in interest rates constitute the most important market risk for the Company.

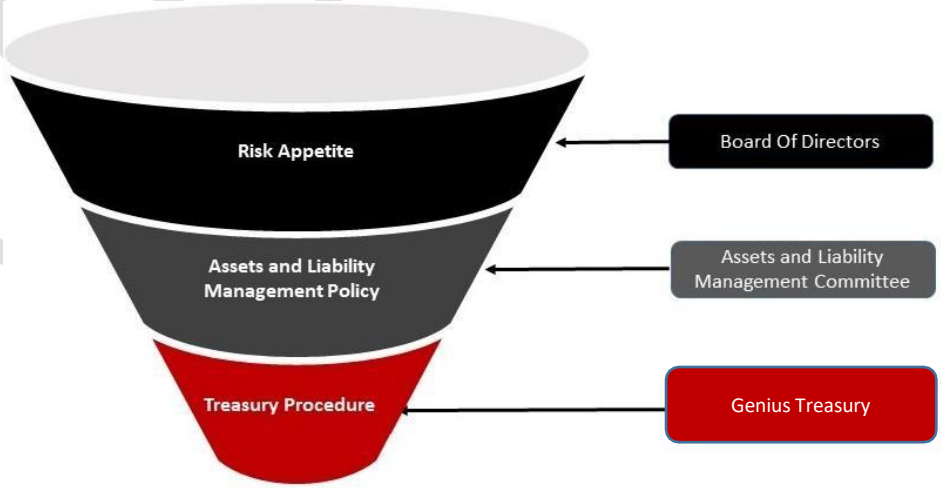
- **Market Risk Management Approach**

Movements in interest rates should be closely monitored. Further, the Company maintains an adequate Net Interest Margin (NIM) so that increases in interest expenses can be absorbed. The company's market risk management should be operationalized through ALM Policy and Treasury procedure and Board-approved Risk appetite limits.

7.3 Liquidity Risk

Liquidity risk is the risk of only being able to meet liquidity obligations at increased cost or, ultimately, being unable to meet obligations as they fall due. In the case of the Company, this relates mainly to the ability to meet refund of deposits obtained from the public as they fall due and the settlement of installments on bank and other borrowings.

- **Liquidity Risk Management Approach**



Special attention should be given on the liquidity of the Company as it provides critical defense against this and several other risks such as reputation, compliance, and financial risks. The company should maintain a conservative outlook towards managing Liquidity Risk, which is governed by the Board approved ALM Policy and appropriate Risk Appetite Limits. Although the mismatch in assets and liabilities in terms of maturity is widely prevalent in the industry, in view of the composition of the portfolio of the Company, this mismatch should be mitigated to a satisfactory condition given in the market conditions. The company's liquidity risk management is operationalized through ALM Policy and Treasury procedure and Board-approved Risk appetite limits.

7.4 Operational risk

Operational risk is the probability of loss occurring from the internal inadequacies of a firm or a breakdown in its controls, operations, or procedures.

- **Operational Risk Management Approach**

Sound operational risk management policy covering awareness building and operation risk identification and treatment should be put in place to be followed by staff to mitigate operational risks and the effectiveness of the same is assessed on a continuous basis. In this context, the Value driven culture which is rigorously promoted across all levels of Commercial Credit strives to ensure that all employees who are self-disciplined, plays a key role. The company's operational risk management is operationalized through Operation Risk Management Policy and Board-approved Risk appetite limits.

7.5 Reputational Risk

Reputational risk is the risk of loss resulting from damages to the Company's reputation, in lost revenue, increased operating cost, capital or regulatory costs; or destruction of shareholder value, consequent to adverse publicity arising from an event that would hurt its reputation. For Commercial Credit, this relates to the borrowers' negative perception about the Company and a loss of confidence on the part of depositors. Further, with the emergence of the Company as a major player among NBFIs, it is critical that due attention is given to safeguard the reputation the

Company has earned among all stakeholders. In today's highly interconnected world with the capability to communicate rapidly, an excellent reputation carefully built over a long period could be at risk instantly.

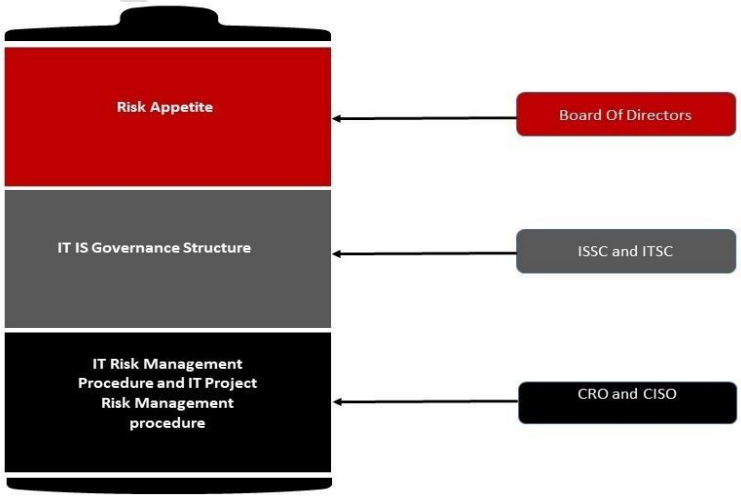
- **Reputational Risk Management Approach**

Strong Corporate Governance and Risk Management practices should be promoted across all levels of the Company to manage the reputational risks. Promotion of the Value driven culture within the organization. The Company pays close attention to ensure that there is no reputation-reality gap for any stakeholder group of Commercial Credit. The RMT should assess any event to determine the risk it has on the reputation of the company and report to the BIRMC. The risk should be addressed according to Anti Money Laundering and Terrorist Financing Policy, Communication Policy, Compliance Policy, Ethical Framework, Whistle Blower Policy, and the Customer Complaint Handling Policy.

7.6 Information Technology (IT) Risk

IT Risk Management is the risk of disruption associated with the use, ownership, operation and adoption of IT in relation to customer data, business processes and critical systems. With the growing needs of the business, the focus on managing IT risks is intensified in recent years with an ever-increasing emphasis on strengthening IT governance to align with CBSL directives as well as globally accepted best practices.

- **Information Technology Risk Management Approach**



IT Risk Management, IT Project Risk Management, and Information Security Risk Management fall within the purview of the Chief Risk Officer (CRO) as part of the second line of defense. Information Security Management is under the responsibility of the Chief Information Security Officer (CISO) as part of the first line of defense. The company's IT IS risk management is operationalized through IT IS Governing Structure and Board-approved Risk appetite limits. The Company should establish a governance of information security and Information Security risk management, by establishing an Information security team which is headed by the Chief Information Security Officer (CISO) and an Information Security Steering Committee (ISSC) and Information Technology Steering Committee (ITSC) which reports to the BIRMC and is responsible for managing risks relating to information security.

7.7 Strategic Risk

Strategic risk can be defined as risks that affect or are created by the company's business strategy and strategic objectives. Strategic risk could also arise due to changes in the competitive landscape or regulatory framework or ineffective positioning in the microeconomic environment. The failure to execute strategy or failure to take effective actions address under-performance could also increase the exposure to Strategic Risk.

- **Strategic Risk Management Approach**

  The primary means of managing strategic risk is through a Board-approved Strategic Plan prepared annually to outline the future direction of the company through a set of long-term goals, objectives and priorities alone with the actions needed to achieve them in line with the company's purpose. It is the key document used by the leadership to prioritize the allocation of resources, to strengthen the company's competitive position. The risk should be addressed according to Budgetary Procedure, and Capital Planning Procedure

7.8 Human Resource Risk

Human resource risk refers to the potential risks and challenges associated with managing an organization's workforce. These risks can have a significant impact on an organization's ability to achieve its goals and objectives. Human resource risks include but are not limited to;

- Employee turnover
- poor employee management practices
- unexpected temporary leave
- management error/incompetence
- disability (temporary or permanent)
- Death

- **Human Resource Risk Management Approach**

The human resource risk should be address according to the HR Policy and the risk appetite statement of the company.

7.9 Capital Risk

For a financial institution capital is a buffer against insolvency. It is available to absorb unforeseen losses so that the Company can remain in business. The more capital the Company has relative to the risks it takes, the more confident the stakeholders are that it will meet its obligations to them. Capital adequacy risk arises from Company's inability to maintain the required amount of capital which is perceived to be adequate to absorb the unexpected losses.

- **Capital Risk Management Approach**

The company's capital risk management is operationalized through capital planning policy and Board-approved Risk appetite limits.

The Company's capital management objectives can be summarized as follows:

- Maintain sufficient capital to meet minimum regulatory capital requirements.
- Hold sufficient capital to support the Company's risk appetite.
- Allocate capital to businesses to support the Company's strategic objectives.
- Ensure that the Company maintains capital in order to achieve debt rating objectives and to withstand the impact of potential stress events.

7.10 Legal/ Regulatory Risk

Legal/Regulatory risk is the risk of loss caused by non-compliance with existing or new legislation or supervisory regulations, disadvantageous changes to existing laws or supervisory regulations. Furthermore, legal risk includes losses due to ambiguity of laws or unfavorable contract clauses and loose contracts.

- **Legal Risk Management Approach**

An independent compliance function should be established by the BIRMC to overlook laws and regulations relating to the company. A compliance policy should be established to manage the compliance function with an appropriate compliance officer's mandate.

7.11 Environment, Social and Governance (ESG) Risk

ESG risk is non compliance with the regulations and best practices of the effectively manage environmental, social and governance (ESG) risks associated with the operation and to assist businesses that are greener, climate friendly and socially inclusive. Identification of Priority Sectors for Sustainable Finance Activities to prioritize granting funding and reporting on sustainable finance activities to ensure sustainable savings products and sustainable loan products, including sustainable leasing products and to encourage supporting green and socially inclusive projects and issue guidance and operational tools, as required. Governance risk involves ensuring that the company is managed ethically and transparently. This includes issues such as executive compensation, avoiding conflicts of interest, and maintaining high standards of integrity in financial transactions. Governance risk also includes adherence to financial regulations and compliance with industry standards. Failure to comply can result in legal and reputational consequences.

- **ESG Risk Management Approach**

Risk management team is requested to identify and evaluate ESG risks, and risks relating to sustainable business activities, considering the nature, scale, complexity and

interconnectedness of their operations and assess the magnitude and materiality of such risks. Risk management team should implement effective risk management practices and internal controls to mitigate the identified risks, and incorporate ESG risk management to the entire decision-making processes.

7.12 Anti Money Laundering (AML) Risk

The Financial Intelligence Unit of Sri Lanka (FIU) has issued Customer Due Diligence Rules applicable to institutions engaged in "Finance Business" activities which include Non-Bank Financial Institutions such as Commercial Credit and Finance PLC. The rules require that every Financial Institution should identify and analyze and design effective implantation of policies and procedures to mitigate identified risks related to ML/TF. This procedure has been prepared to evaluate and mitigate risk of Anti Money Laundering activities (AML), Terrorist Financing activities (TF) and identification of Politically Exposed Persons (PEP) on a risk based approach.

- **AML Risk Management Approach**

AML risk should be managed according to the Anti Money Laundering and Terrorist Financing Policy.

7.13 Model Risk

Model risk refers to the potential for financial loss or other adverse consequences resulting from the use of mathematical models, such as statistical, financial, or machine learning models, to make decisions or predictions in various fields, including finance, business, and engineering. This risk arises from the fact that models are simplifications of complex real-world systems, and their accuracy and reliability can be limited by various factors.

- **Model Risk Management Approach**

Model risk should be managed according to the Model Risk Management Framework and Model Validation Policy.

8. Risk Appetite Statement (RSA)

The RAS sets the tolerance for risk-taking in the company's operations within the company's risk-bearing capacity. Risk limits and risk profile assessment are other key elements in the implementation of the company's risk appetite and the risk appetite should address the risk factors related to the company mainly Credit risk, Liquidity, Market, Operational, Compliance, reputation, IT and etc.

The objectives of the RAS are the following

- To provide a clear direction of the company to define the risk-taking at the high level.
- To increase understanding of the company's material risk exposures and raise risk awareness across the organization.
- To support the Board of Directors and the senior management in planning, formulating and executing strategic business decisions to achieve the long-term targets of the company.
- To provide tools for the Board of Directors and senior management to continuously monitor and align the company's actual risk profile with the risk appetite.

The following responsibilities are applicable in relation to the RAS

- The board of directors of the Company is responsible for setting limits and tolerance levels of the company and review the risk appetite statement of the Company annually.
- The BIRMC should monitor the Company's adherence to the RAS, and make necessary changes to capture changes in the company's strategic priorities, operating environment, and risk profile
- Chief Risk Officer is responsible for prepare the risk appetite statement monthly basis and present to the BIRMC for review.
- Management of the company is responsible to use the risk appetite statement as a board approved risk taking level of the company when strategic planning, operations, setting policies and procedures.
- The senior management is responsible for providing input for setting risk limit and any variance if any.

The RAS should include the following features,

- **Monitoring Frequency**

It should be contained the period that is considered for the calculation. It can be monthly, quarterly, semiannually or annually.

- **Description of the Risk**

The risk should be descripted and the method of calculating should be stated such as formula or any specific factors

- **Risk Tolerance**

Risk tolerance is the amount of risk that the company is comfortable taking than the risk limits of the company or the degree of uncertainty that the company is able to handle.

- **Performance of the Reporting Period**

When repoting the performance for each risk factor ratios should be presented as annualized figures.

- **Risk limits (Targets)**

Risk limits should be decided based on the corporate plan and industry practices. The limit sets the boundaries for the accepted level of credit, market, liquidity and operational risk within the established risk appetite

- **Variance**

Variance should be calculated as the difference between the target and the actual performance of the company for the considered period.

- **Format of the RAS**

Risk appetite statement need to be presented in the format given in the Annexure 2 below.

- **Review of the RAS**

RAS should be reviewed once a year or sooner if required, due to any change in risk environment, and recommend to the Board of Director's approval through BIRMC

9. Business Continuity Management

Business Continuity Management is a significant aspect of operational risk management. The company should therefore develop a Business Continuity Plan to ensure the company's ability to

operate on an ongoing basis and limit losses in the event of severe business disruption caused by operational disruption, natural disasters, epidemics or terrorism.

Develop detailed business continuity plans for implementing the recovery strategy. Business Continuity Plan should:

- Identify the risks to critical business processes, including those where there is dependence on external vendors or other third-parties, for which rapid resumption of service would be most essential

- Assess the potential impact of various disruption scenarios, including a major operational disruption, to which the company may be vulnerable, commensurate with the size and complexity of its operations

- Establish recovery objectives and priorities in the event of disruption. These objectives should be influenced by the likely impact of the disruption to the broader financial system

- Include identification of alternative mechanisms for resuming service in the event of an outage. Particular attention should be paid to the ability to restore electronic or physical records that are necessary for business resumption. Where such records are maintained at an off-site facility, or where operations must be relocated to a new site, care should be taken that these sites are at an adequate distance from the impacted operations to minimize the risk that both primary and back-up records and facilities will be unavailable simultaneously

- Develop communication strategies, in the event of a disruption, within the company and with relevant third parties, including regulators in other jurisdictions where a branch operates

- Review periodically company's disaster recovery and business continuity plans so that they are consistent with the current operations and business strategies

- Test these plans periodically with all relevant personnel to ensure that the management would be able to execute the plans in the unlikely event of a severe business disruption

- Subject these tests to audit review and address any deficiencies that are identified
- A comprehensive Disaster Recovery Plan should be in place in preparation of contingent risk incidents.

10. Stress Testing

Stress testing should be carried out to assess the impact on credit, earning, liquidity & capital according to the stress testing policy of the company.

End of the Document

Recommended by the BIRMC on 11.01.2024
Approved by the BOD on 31.01.2024

Annexure 1: Risk Management Process

A.1.1 Identification of Risk Events

Identification of risk sources/ risk events provides a basis for systematically examining changing situations to meet its objectives. The risks of the company should be identified through the Risk Control Self Assessment (RCSA), analytics and examinations by the process owners and the CRO. These risks can be identified from various sources including audit reports of internal audit, CBSL onsite audit and external audit, actual loss experience and regulatory reviews.

A.1.2 Rating of risk events

Self-rating of risk events is designed to bring together all of the findings of the review and to provide senior management with concise feedback regarding the overall quality and status of the controls. Identified risks should be assessed to grade the risk based on the overall risk.

Evaluation should be done as follows.

Parameters for evaluating, categorizing, and prioritizing risks typically include

- risk likelihood (i.e., the probability of risk occurrence),
- risk impact (i.e., the impact and severity of risk occurrence),

The risk likelihood and impacts identified will mapped using the risk Matrix below.

		Likelihood			
		Remote	**Possible**	**Likely**	**Cer**
Impact	**Low**	1) Accept	2) Accept/Control	3) Accept/Control	4) A
	Medium	2) Accept/Control	4) Accept/Control	6) C	
	High	3) Accept/Control	6) Co		
	ical	4) Ac			

At risk evaluation risk factors should be assessed and determined in terms of impact of the risk factor as follows

Guidance on Impact Rating	
Scale	Rating
4	Cri
3	
2	

At risk evaluation risk factors should be assessed and determined in terms of likelihood of the risk factor as follows

Guidance on Likelihood Ratings		
Scale	Rating	Explanation
4	Certain	Very high possibility to occur
3	Likely	Likely to occur
2	Possible	Might occur at some time
1	Remote	Very low possibility to occur

Overall risk score is decided based on points generated by likelihood and impact as follows,

The evaluation of risks is needed to assign relative importance to each identified risk, and is used in determining when appropriate management attention is required. The following risk categories and scores will be used identify prioritize risk.

Overall Risk Category	Overall Risk Score
High Risk	12 to 16
Medium Risk	6 to 9
Low Risk	1 to 4

A.1.3 Identification of Controls

Identification of manual and system controls that have already been implemented to address the identified risks.

A.1.4 Assess the controls

After identifying the controls that have already been implemented, such controls need to be assessed to identify whether those controls are effective to mitigate the risk or not. In addition, it should be assessed to determine whether those controls are working as intended. If there is any lapse in the controls, suitable action should be proposed.

A.1.5 Recording

The risk department should record those risk matters in a register and monitor the identified actions till they come to effective level.

Risks should be documented in the Risk Register. The Risk register will comprise of the risk description, risk treatment, action taken, suggestions and responsible person form management of each risk item.

The risk assessment is done by chief risk officer and he should discuss the identified risks with the relevant risk owners before presenting to the senior management to evaluate their plans to mitigate them.

The risk sheets in the Risk Register need to be used to record the identified risks

Risk Description; Description of the risk factor in detail.

Risk Type (Inherited); Percentage of the inherited of the risk factor. Percentage is decided by the risk owner and the CRO.

Risk Type (Control); Percentage of controllability of the risk. Percentage is decided by the risk owner and the CRO.

Risk Category; Each risk need to be categorized as Credit risk, Market risk, Liquidity risk, Operational risk or Reputational risk for risk management purpose.

Overall Risk; Total risk of the risk factor will be arrived based on the impact and likelihood of the risk, as explained in 3.2 below.

Impact; Impact is made to the business by risk factor. The impact of the risk need to be evaluated by risk owner and CRO to decide the impact based on chart given in 3.2 below

Likelihood; Likelihood of the occurrence of the risk factor. The likelihood of the risk need to be evaluated by risk owner and CRO to decide the impact based on chart given in 3.2 below

Risk treatment; for each risk factor should be defined as explained in 3.3 below.

Action taken; Action taken by the management to mitigate the risk.

Suggestions; Actions to improve the process

Responsible person; risk owner of each risk factor responsible for the risk mitigation plan.

Residual risk ; the risk item after implementing the mitigation activities are acceptable to the company according to the risk appetite of the company. Such decision can be taken by the Chief Risk officer

A.1.6 Design a Mitigation Strategy.

The risk matrix produces a risk rating score which will enable risks to be treated using one or more of the following treatments:

(1) ***Control*:** Taking active steps to minimize risks;

(2) **T*ransfer***: Reallocating the risk to external party to lower the risks;

(3) ***Acceptance***: Acknowledgment of risk but not taking any action,

(4) **Termination:** Agree that the risk is too high and do not proceed with the activity

Each risk factor should be assigned to a specific person or persons to take responsibility over the implementation of risk mitigation plan.

A.1.7 Review and Reporting

Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place. This activity may result in the discovery of new risks or new risk-handling options that may require re-planning and reassessment.

The risk review should cover the following areas.

(1) Updated of the risk register and risk status;

(2) Updated assessments of risk likelihood

(3) Updated list of actions taken to handle risks; and

(4) Risk mitigation plans.

The CRO should evaluate adherence of the risk management process against its process description, standards, and procedures, address noncompliance and discuss with the management to improve the remedial actions.

Risk mitigation activities which have been taken by the management should be reported to the BIRMC as a summarized report (Risk Dashboard) by chief risk officer at BIRMC meetings or sooner when he believes that any risk factor is significant. These reviews will include a summary of the

most critical risks factor, key risk parameters (such as likelihood and impact of these risks), and the status of risk mitigation efforts.

Chief risk officer should follow up recommendations that are made by the BIRMC and report them timely.

The Chief risk officer has to periodically monitor the RCSA, including results of testing and corrective action tracking. Evidence of this monitoring should be maintained.

RCSA results have to be incorporated into the quarterly operational risk report. High level information has to be sent to the board of directors and the senior management.

A.1.8 Control Testing

Frequent internal audit testing – the effectiveness of self-assessment is evaluated in terms of the quality and reliability of the assurances the process provides to certifying officers. Therefore, internal audit should test selected controls to evaluate the quality of the assertions reported through the self-assessment program. In such instances, internal audit's testing work product should be documented 'outside' the self-assessment program used by process owners.