IndiaFirst Life Insurance Company Limited

Risk Framework & Policy

Version	Month	Approved by	Remarks
1.0	Mar-18-2010	Board	Meeting of the Board of Directors held in March 2010.
1.1	Jun-28-2011	Internally	Showing RMC and ALCO as merged entity.
1.2	Nov-08-2016	Risk Management Committee	Inclusion of Risk Tolerance limit & Inclusion of Project risk under Risk Management approach
1.3	Nov-07-2017	Risk Management Committee	Inclusion of Cyber Risk under Risk Management approach
1.4	Feb-06-2019	Risk Management Committee	Reviewed with no change.
1.5	Feb-02-2021	Risk Management Committee	• Incorporated section providing overview on Documentation Control and Classification. • Classification of risks in to four types in clause no. 3 on Risk Management Approach, and giving reference to Outsourcing Policy, Anti-Fraud Policy, Information & Cyber Security Policy and PPI Policy. • Modification done in the Risk Management Governance structure in clause no. 4 on Risk Governance Framework • Incorporated separate sub-clause on Review of policy in clause no. 4 on Risk Governance Framework.
1.6	Jan-28-2022	Risk Management Committee	Reviewed with no changes
1.7	Oct-17-2022	Risk Management Committee	• The risk management objective is changed to align with the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 • The size and composition and quorum of the Risk Management Committee is changed to align with the Listing Regulations

Document Control and Classification:

Policy Name:	Risk Framework & Policy	
Department:	Risk Management	
Document Owner:	Chief Risk Officer	
Document Reference/No.:	Risk Framework & Policy Version 1.7	
Information Classification:	External	
Prepared by	**Reviewed by**	**Approved by**
Risk Function 17-Oct-22	Chief Risk Officer	Board of Directors October 18, 2022

INDEX

1 Purpose of Document

The purpose of this policy is to describe the risk framework for IndiaFirst Life Insurance Company Limited ("**Company**") which covers company's overall approach to all risks. The [Company's] Risk Framework is the structure of risk management policies, formal committees and reporting processes in place across the firm, which enable the Board to draw assurance that all risks are being appropriately identified and managed, and that an independent assessment of risks is being performed. It is understood that as the company sets its sail on a long journey, its risk framework will also evolve over time.

The Risk Framework, as approved by the Board, has been implemented by the Risk Management Committee (RMC).

2 Risk Management Objectives

1. The main objective of this Risk Management policy is to ensure sustainable business growth with stability and to promote a pro-active approach in reporting, evaluating and resolving risks associated with the business. In order to achieve the key objective, the Policy establishes a structured and disciplined approach to Risk Management, including the development of the Risk Register, in order to guide decisions on risk evaluating & mitigation related issues. The Policy is in compliance with the Regulation 17(9) of Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, as amended (the "**Listing Regulations**"),provisions of Companies Act, 2013, as amended and the Corporate Governance Guidelines dated May 18, 2016 by the Insurance Regulatory and Development Authority of India ("**IRDAI**") which requires the Company to lay down procedures about risk assessment and risk minimization.

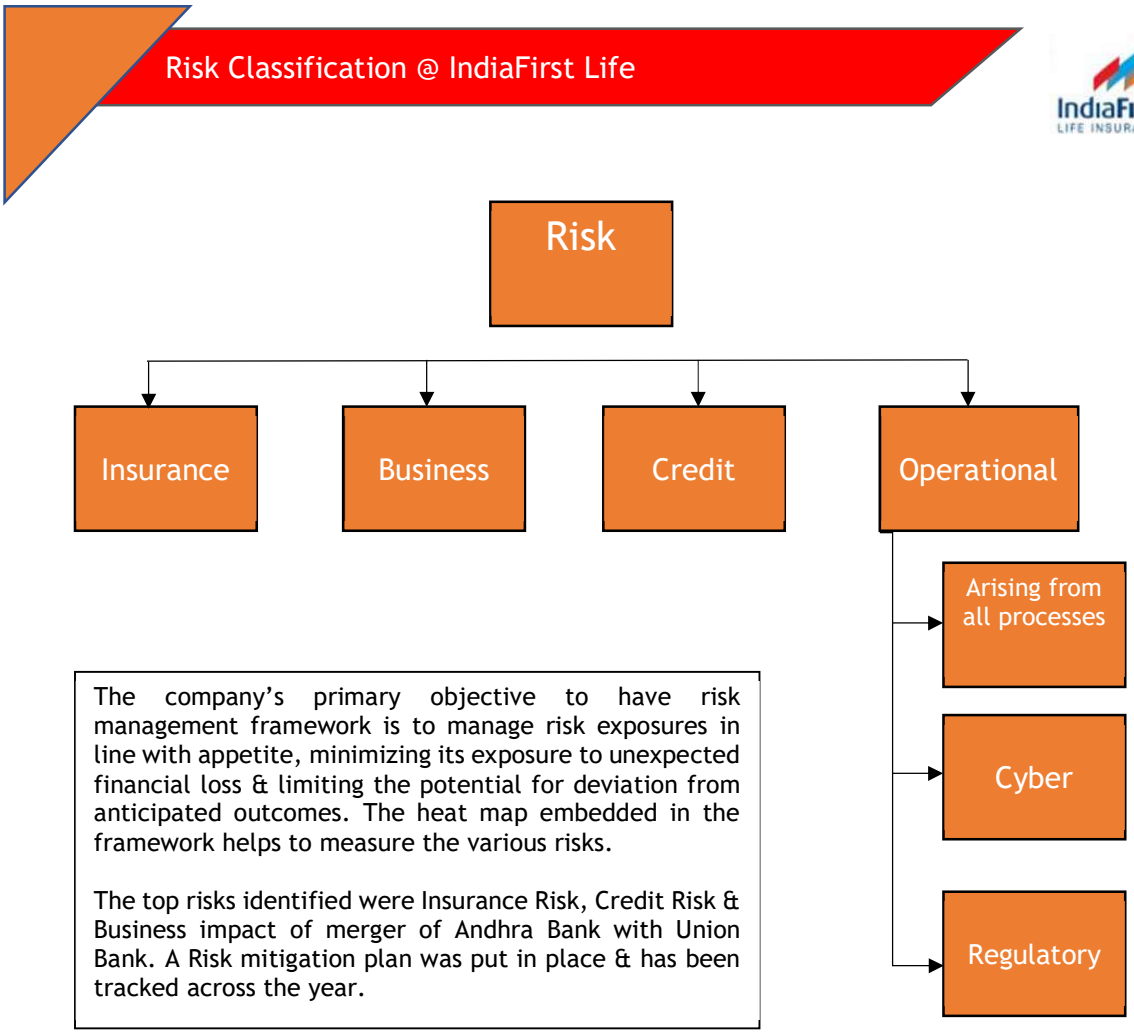
3 Risk Management Approach

The Company's business involves the acceptance and management of risk. The Company is exposed to insurance, market, credit, liquidity and operational risks and the Risk Framework is designed to ensure that all significant risks are identified and managed. At IndiaFirst, risk management is the process by which the company determines how much risk of each type it is willing to be exposed to, determines the policies it will adopt for managing these risks and ensures implementation of these policies. Risk management is the responsibility of the entire management team and staff of IndiaFirst. They are supported in this role by the Sub Risk Management Committee ("**RMC**"). Risk Management function will be the decision making authority and the executor of the risk framework, within the confines of the regulatory and strategic directives of the company, and will work under the guidance of the Board of Directors and RMC on various policy matters. In addition, Internal Audit has responsibility for reporting to the Audit Committee the company's adherence to internal systems and controls, procedures and policies (which include risk and compliance frameworks). This structure provides "three lines of defense" in the identification, assessment and mitigation of potential risks to the organization.

A. Risk classification and its Management

The Company has classified various risks in to four types as below:

1. Insurance
2. Business
3. Credit & Investment
4. Operational



i. Insurance Risk:

Insurance risk is the risk arising from higher claims being experienced than anticipated and is implicit in company's insurance business and arises as a consequence of the type and volume of business written and the concentration of risk in particular policies or groups of policies subject to the same risks.

- The Company's insurance risk policy sets out the overall framework for the management of insurance risk. As part of the framework, a structure of delegated pricing and underwriting authorities is in place. Pricing is based on assumptions, such as mortality and persistency, which have regard to past experience and to trends. Insurance exposures are limited through reinsurance. Overall, the company seeks to be prudent in its acceptance of insurance risks by establishing strict underwriting criteria and limits.

- The underwriting policy is clearly documented, setting out risks which are unacceptable and the terms applicable for non-standard risks.
- Reinsurance is used to reduce potential loss to the company from individual large risks and catastrophic events.
- The Company has a documented reserving policy setting out the basis on which liabilities are to be determined using statistical analysis and actuarial experience. This policy is in line with locally established actuarial techniques, relevant regulation and legislation. The appointed actuary will assess the reserving policy on a regular basis in accordance with IRDA guidelines.

ii. Business Risk

Business risk that is faced by the insurance company is like normal risks faced by other businesses.

iii. Credit & Investment Risk

Financial risk comprises of market risk, liquidity risk and credit risk.

Market Risk is the potential losses in the value of invested capital as a result of changes in market prices due to fluctuations in interest rates, share prices, exchange rates and other relevant market prices. The company manages market risk using the following methods:

Asset Liability Matching

As per IRDAI Corporate Governance Guidelines dated 18th May 2016, All insurers shall constitute Asset Liability Management Committee ("**ALCO**") for the life insurance business.

- Accordingly, the company has formulated an ALCO for an ongoing process of formulating, implementing, monitoring and revising strategies related to assets and liabilities to achieve an organization's financial objectives, given the organization's risk appetite, risk tolerances and Business profile.
- The ALCO lays down the framework to ensure that the company invests in a manner which would enable it to meet its cash flow needs and capital requirements at a future date.
- The company has an Asset Liability Management Policy that takes in to account the company's asset-liability relationships, overall risk tolerance, its risk and return requirements, solvency position and liquidity requirements. The meeting of ALCO is conducted in accordance with Terms of Reference of ALCO,

Credit Risk is the risk of loss if a borrower or counter-party fails to perform its financial obligations to the company.

- The Company's credit risk policy defines the overall framework for managing credit risk.
- The Company has put in place a Credit Research and Review process. The team carries out credit review of companies under the portfolio and place a report to Investment Committee. The periodicity of review is at least twice a year or at the time of any significant credit event in the company.
- The framework of credit review process is approved by Investment Committee
- Significant areas where the company is exposed to credit risk are

- The company holds corporate bonds to back part of its insurance liabilities. Significant exposures are managed by the application and regular review of concentration limits, with allowance being made in the actuarial valuation of the insurance liabilities for possible defaults.
- The company will limit its exposure to insurance risk by ceding part of the risks it assumes to the reinsurance market. To limit the risk of reinsurer, default the company operates a credit rating policy when arranging cover and sets minimum criteria when selecting a reinsurance partner.
- Managing of credit risk is done in accordance with Investment Policy

Liquidity Risk is the risk that the company, though solvent, does not have sufficient financial resources available to enable it to meet its obligations as they fall due, or can only secure them at excessive cost. A degree of liquidity risk is implicit in the company's businesses. Liquidity risk arises as a consequence of the uncertainty surrounding the value and timing of cash flows.

- The company's finance function is responsible for managing the banking relationships, capital raising activities, overall cash and liquidity position and the payment of dividends. The Company seeks to manage funds and liquidity requirements on a pooled basis and to ensure the company maintains sufficient liquid assets to meet a prudent estimate of its net cash outflows.
- In addition, it ensures that, even under adverse conditions, it has access to the funds necessary to cover surrenders, withdrawals and maturing liabilities. In practice, most of the company's invested assets are marketable securities. This, combined with the fact that a large proportion of the liabilities contain discretionary surrender values or surrender charges, reduces the liquidity risk.
- Managing of liquidity risk is done in accordance with Investment Policy

iv. Operational Risk

Operational risk is the risk of direct loss resulting from inadequate or failed internal processes, people and systems or from external events, which include legal and compliance risk and fraud. Risks related to Marketing and Distribution, reputational risk and strategic risks are also covered under operational risks.

All business managers are required to confirm regularly the adequacy of controls over operational risks to the RMC and the Audit Committee. Significant control issues which business areas identify are escalated to the Sub Risk Management Committee , which will oversee their resolution. There are a number of categories under which operational risk and its management across the company can be considered, and these are outlined in the following paragraphs.

1, People Risk

The company is potentially exposed to the risk of loss from inappropriate actions by its staff. The risk is actively managed by business management and human resource (HR) functions.

- Recruitment is managed centrally by HR function, and all new recruits undergo a formal induction program.
- All employees have job descriptions setting out their accountabilities and reporting lines, and are appraised annually in accordance with agreed performance management frameworks and half-yearly reviews.
- Employees are provided with appropriate training to enable them to meet the relevant regulatory requirements.
- Risks relating to health and safety and other legislation are managed through the provision of relevant training to all staff.

2. Outsourcing Risk

The company is potentially exposed to the actions or failure of suppliers contracted to provide services on an outsourced basis.

- The required minimum standards of control for outsourced arrangements are set out in the company's outsourcing and key supplier policy.
- The Company has formed an Outsourcing committee in accordance with IRDA regulations to oversight the outsourcing of activities of Company. The Company has an Outsourcing Policy in place and management of Outsourcing Risk is managed by Outscoring Committee in accordance of Outsourcing Policy.

3. Legal and Compliance Risk

Legal risk is the risk of loss from unclear or deficient product documentation; inadequate documentation in support of material contracts such as reassurance treaties; the incorrect interpretation of changes in regulation; employment related disputes and claims; and commercial disputes with suppliers.

- The risks are actively managed through Legal and Compliance function of the Company's Risk Management department, which mandatorily signs off on each and every legal or binding contract that the company enters into and also defines minimum standards of control to be applied to minimize the risk of loss.

Compliance risk within the company relates to the risk of non-adherence to legislative requirements, regulations and internal policies and procedures.

- Responsibility for ensuring adherence to relevant legal and regulatory requirements is vested in individual business managers.
- The Company's Legal & Compliance function oversees Company's compliance with regulatory requirements and standards, providing policy advice and guidance and oversight of compliance arrangements and responsibilities.
- This shall include a formal process of monitoring and control of Brand Compliance, Process Compliance, Etiquette Compliance and Code of Conduct Compliance.

4. Project Risk- A risk is any factor that may potentially interfere with successful completion of the projects

Identification of Risks

Identify different milestones & probable risk attached to the project basis brainstorming session with the team members of the various departments & past experience

Assessing of Risks

Assess & identify the impact the various risks which are identified at programme & operational level and check if the same are with the tolerance limit or beyond.

Mitigation of Risks

Risk management planning needs to be an ongoing effort that cannot stop after a qualitative risk assessment. Risk mitigation strategies and specific action plans should be incorporated in the project execution plan.

Risk Management plan should include,

- Characterize the root causes of risks that have been identified and quantified in earlier phases of the risk management process.
- Identify alternative mitigation strategies, methods, and tools for each major risk
- Evaluate risk interactions and common causes
- Select and commit the resources required for specific risk mitigation alternatives

Event

Event risk relates to the potential for loss arising from significant external events such as terrorism, financial crisis, major changes in fiscal systems or disaster. Typically, such events have a low likelihood of occurrence, a material impact and can be difficult to prevent. The company's risk mitigation will focus on minimizing the business disruption and potential financial loss which may ensue from such an event.

- This shall include maintaining a framework for the management of major incidents, the maintenance and regular testing of detailed business, technical and location recovery plans (Disaster Recovery Plan and Business Continuity Plan) and the provision of insurance cover for the loss of buildings, contents and information technology systems and for the increased cost of working in the event of business disruption. This includes escrow arrangement for critical Systems Code in case of vendors getting out of business and Annual Maintenance Contracts for critical systems and hardware.

5. Fraud Risk

The company is potentially exposed to the risk of internal fraud, claims-related fraud, and external action by third parties.

- The company has an Anti- Fraud policy. The Fraud Control unit is responsible for administering the same & makes periodic reports to the Vigilance & Ethics Committee which files a half yearly report to the Audit committee
- The company also has a whistle blower policy in place.
- The fraud related risks are managed in accordance with Anti-Fraud Policy

6. Technology Risk

- The company places a high degree of reliance on IT in its business activities. The failure of IT systems could potentially expose the Company to significant business disruption and loss. The Company has an Information and Cyber security policy to manage the technology related

risks that defines the standard guidelines and overall framework for implementing and sustaining such compliant and effective security program aimed at protecting the confidentiality, integrity and availability of information assets.

- The Company also has Business Continuity Management policy to ensure continuity of critical operations and provide services, support to all its customers and stakeholders within a reasonable timeframe and with minimal disruption in case of any disaster.

7. *Cyber Risk-* means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems

   Cyber security in financial sector has gained importance, more so with the advent of technological innovations. The cyber security related risks in managed in accordance with Information and cyber security policy.

8. *Reputational Risk*

   The Company is cognizant of the impact of any of its decisions or activities in the marketplace and clearly recognizes the potential implications on not only its own reputation but also on its shareholders' reputation.

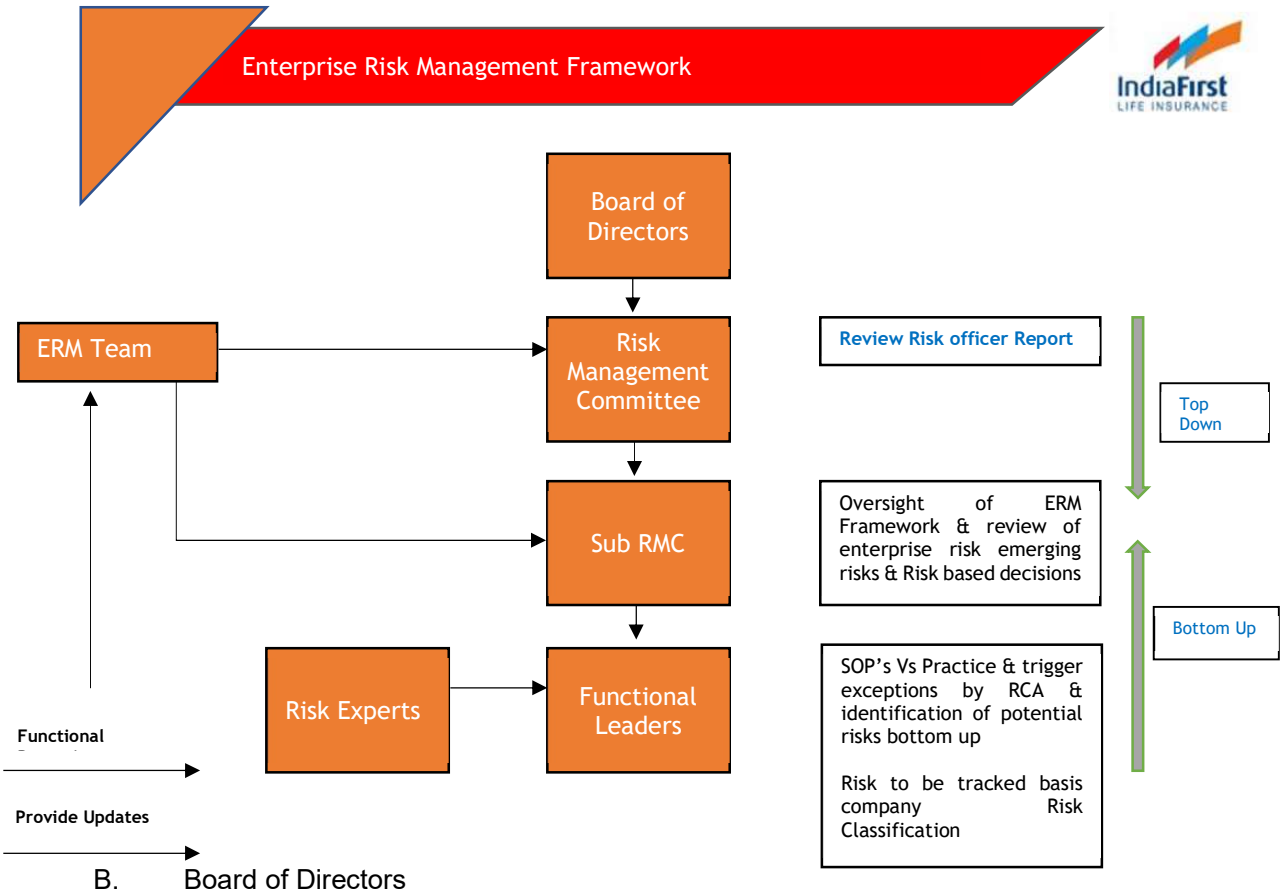
   - The Company has a clearly defined media policy and procedures in place for managing matters that may have reputational implications, to ensure that IndiaFirst's position is correctly understood.
   - The Company has Policy for Protection of Policyholder's Interests (PPI) to ensure interests of policyholders are protected and to have policyholder centric governance by insurers with emphasis on grievance redressal.
   - The Company, as a matter of policy, puts customer first in every act in order to prevent mis-selling which is quite rampant in the marketplace.
   - The company has put in place the Product IVR and verification calls which are additional checks in the new business process that proactively seek confirmation from customers of their choice of plans and understanding of it.

4 Risk Governance Framework

A. Committee Structure

RMC, on behalf of the Board, will oversee the risk management framework. The RMC will meet quarterly to have the necessary focus and time on risk management reporting process to the Board. The RMC will be chaired by a non-executive director of the Board. The governance structure outlines the organizational structure, the hierarchy and the scope of responsibilities of all the governance bodies involved in the risk management function.
The Company's risk management governance structure involves the Board of Directors (Board), the Risk Management Committee (RMC), the ERM (Enterprise Risk Management) Team, the Sub RMC, the Functional Leaders, Risk Experts as per the diagram depicted below.

The Risk Management Committee will seek guidance from Sub RMC, as needed, and provide inputs on risk identification, assessment and mitigation process.



B. Board of Directors

The Board will provide risk management supervision on the extent to which management has established effective risk management process in the Company by reviewing company's portfolio of risk and against its risk appetite. The Board will get an appraisal of the most significant risks from the RMC and will provide feedback on whether the management is in a position to respond to them in an appropriate manner. The Board will be assisted by the RMC in supporting and executing on the risk identification, assessment and mitigation plan.

C. Risk Management Committee (RMC)

The constitution of the RMC has been approved by the Board of Directors and any new appointment or removal of any member of the RMC shall also be approved by the Board.

All the decisions taken by the Risk Management Committee shall be recorded and the same will also made available for verification and audit by the internal auditors and the appointed concurrent auditors, if any.

The composition of the Risk Management Committee shall be as follows.

Chairman	Non-executive Director (such director shall be appointed by Bank of Baroda).
Members	At least four directors
Secretary	Company Secretary to act as Secretary to the Committee
Size and Composition	The RMC shall have a minimum of three members with majority of them being members of the board of directors, including at least one independent director or any other composition in compliance with applicable law. The Chairperson of the RMC shall be a member of the board of directors and senior executives of the listed entity may be members of the committee
Attendance	The Deputy CEO, The Chief Financial Officer, Chief Operating Officer, Chief Risk Officer and Appointed Actuary will attend the meeting. CEO will be a member of the Committee. The Committee may invite any person to be in attendance to assist in its deliberations.
Frequency of Meetings	The Committee should meet at least once in every quarter and shall report regularly to the Board.
Quorum	The quorum for a meeting of the RMC shall be either two members or one third of the members of the committee, whichever is higher, including at least one member of the board of directors in attendance.
Appointment and removal of directors	Any appointment/removal of any member of the RMC shall be approved by the Board.
Reporting to the Board	The Risk Management Committee shall present: 1. An analysis and a report to the Board on the status of risk management process, current risk assessment and mitigation plan at least on a quarterly basis

2. Future outlook of emerging risks to enable the Board to look at possible policy changes and strategies.
3. the Minutes of the Risk Management Committee will also be placed before the Board

D. Risk Management Function

The Chief Risk officer (CRO) on behalf of the Risk Management Function is the main driver behind the implementation of the Risk Management Framework in all its aspects. The Job and Role of the Chief Risk Officer includes the following:

The CRO will be responsible for the identification, measurement and mitigation and follow-up of the controls on the company-wide risks to assure the achievement of goals and objectives through effective risk management. More specifically, he will:

- Develop and maintain comprehensive risk management policy, governance, framework and guidelines
- Together with operating heads, drive identification, measurement, mitigation and control of Company-wide risks
- Facilitate development and improvement of risk management know-how, tools, methodologies and systems
- Independent risk review and assessment on products, projects, assets, capital, investment and Company-wide business activities
- Apply global best-practices in the area of risk management
- Supervise and develop risk management personnel in line with immediate objectives and long-term plans

CRO forms the corner stone of the second line of defence, promoting good corporate governance and providing reasonable assurance on integrity and validity of risk measurement and reporting.

CRO will ensure:

- Independent check-and-balance mechanism
- Provide second opinion
- Offer perspective on potential downsides
- Risk reviewer for business/insurance risk
- Central aggregator for financial risk
- Frontline and organizational support for operational risk
- Make risk a management agenda and risk awareness happen throughout the organization
- Strengthen business cases and plans
- Give assurance on the integrity and validity of self-assessment, measurements and KRIs
- Organize and drive the RMC and the Sub Risk Management Committee.
- Invited to the RMC

Member of all or any specific downstream Function

E. Review of the Policy

This policy will be reviewed by the Sub-RMC on annual basis. The Sub-RMC will recommend the changes in the policy to Risk Management Committee for their review and final approval.

5. Risk Identification & Assessment

A. Risk Identification

Responsibility for the identification and management of risk is vested in business management with the functional heads. Sub Risk Management Committee is responsible for ensuring the completeness of risk assessments, the capture of all risk, control weakness and loss data on risk databases, and the adequacy of assessment of risk-based capital requirements.

The Company shall use a standard framework for the identification and assessment of risk. The framework comprises a number of segments, designed to support the identification and assessment of the range of risks that the company may be exposed to. The framework and segments are set out below:

- *Strategic risks* are the risks and uncertainties that arise from, or are associated with, the company strategy and the business environment in which it operates. The company shall review, confirm and document strategic risks on at least an annual basis as part of the development of the annual operating plans. Typically, the risks will be forward looking. The risks should be confirmed by the Board and the RMC.

- *Inherent risks* are generally those risks that may arise from the types of products sold and the investment assets held to meet liabilities. Exposure to inherent risks shall be documented within formal Investment and Product policies. The policies shall also document the framework of controls required to manage exposures to inherent risks and shall be approved annually by the Risk Management Committee.

The nature of Strategic and Inherent risks is such that it is not always possible to fully mitigate the potential for loss should the risk materialize. Accordingly, as part of the evaluation of a firm's risk based capital requirement, consideration shall be given to the risk capital, to be held where appropriate, against these types of risk.

- *Process Risks* are those risks associated with the everyday operation of systems and processes. The company has implemented an Exception Reporting process for deviations from the SOP. *Operational risk* is the potential for loss resulting from inadequate or failed internal processes, people and systems, or from external events. Operational risk shall include matters related to customer care such as new business, ethical selling, underwriting, policy issuance, claims as well as compliance. The company has limited appetite for operational risk in that it does not seek to make a return from taking operational risk and will seek to do all that is commercially feasible to minimise its potential exposure to loss or damage from operational risk events. However, it is accepted that losses due to operational risk do occur as a result of system and process failures, human error and external events. Provision shall be made within operational risk capital for the cost of actions to ensure that business change does not increase company's exposure to operational risk though potential reputational damage, adverse impact on policyholders, financial loss or breach of regulation.

In the context of having limited appetite for operational risk, the company seeks to set a business operating environment such that:

- The company complies with the local legislation and regulation.
- The potential for adverse media coverage, customer complaint or impact on employees following an operational risk event is minimised;
- The potential for policyholders being exposed to financial loss or disadvantage from the materialization of operational risks is minimised;
- Controls shall be kept in place to limit the potential for financial loss to the company to the extent that it is commercially feasible to do so.
- Where possible, the company shall set limits and tolerances on exposures to specific risk areas.

Additionally, a number of policies have been developed for the management of specific aspects of operational risk. These policies shall be periodically audited through Internal Audit.

- *Key Risks & Issues* are those transient matters and issues that require active senior management involvement to ensure that they do not result in loss or reputational damage. Typically, risks falling into this category will be those relating to the failure to manage business change; new business launch; the introduction of new products; or significant regulatory matters. The materialization of the risk could result in financial loss, reputational damage or a breach of regulation.

  Key Risks & Issues shall be identified through a top down/bottom up evaluation and review process, whereby senior managers within the company articulate their key concerns and risks (top down) and operational management identify matters of concern to them (bottom up), with an overall aggregation and analysis of key matters (and resulting management actions) being performed by the respective functional heads. The identification and management of Key Risks & Issues is a key area of focus of the Sub Risk Management Committee.

  Key Risks & Issues shall be assessed with regard to their impact and likelihood of occurrence. The company will use a scale of 1 to 5 to approximate impact and a similar scale to score the probability. In addition to scoring impact and probability of a key risk occurring, the target outcome or desired operating range for the risk shall be identified with mitigation plans being focused to achieve this outcome. An assessment shall also be made of the amount of risk capital required for the residual finance loss that could arise if management actions fail to fully mitigate the risk. The Key Risks & Issues and the status of mitigation plans shall be considered at each meeting of the Sub Risk Management Committee and the Risk Management Committee.

- *Management Information System (MIS)*

  Adequate and appropriate management information is a key tool in the management of risk. Responsibility for the provision of information and its accuracy is vested in business management functions. Sub Risk Management Committee oversees the flow of information on risks, mitigation actions and issues, and confirm that it is appropriate and adequate for risk management purposes.

  The RMC and the Sub Risk Management Committee, and particularly the Chair of each Committee, shall be asked periodically to confirm that they are satisfied with nature of management information received. Company Risk and Compliance, Internal Audit and Business functions may also contribute through their ongoing monitoring activities.

Sub Risk Management Committee shall oversee the management information processes for the company and support the development of management information system and processes for the company. Responsibility for the compilation of board packs is with the Risk Management Committee. The RMC may delegate this task to the Sub Risk Management Committee and may provide the necessary guidance on the development of companywide risk reports to ensure alignment of reporting processes across the company.

B. Risk Tolerance Limit

A measure of how much risk you can handle as an organisation. Risk tolerance is an important component which a Chief Risk officer has decide before assessing degree of risk.

Appetite and Tolerance for all type of risks

IndiaFirst Life has the following level of tolerance for the following type of risks

- Low & Medium for all Operational risks,
- Medium and High for all Regulatory risks
- Medium and High for all Reputational risks
- Medium and High for all Financial risks

Basis on the exposure appropriate measures will be taken towards achieving a high level of risk awareness and establishment of a rigorous risk management system.

Insurance Risk Tolerance Framework:

- The level of tolerance will be determined basis the processes, internal control, Internal Audit, & culture, with in organisation
- Risk tolerance limits for identified risk areas would be also decided basis the following factors:
  - Incidence management & loss data bases, Historical trend analysis data
  - Contingency and business continuity plans for respective processes
- High standards of ethics and integrity,

The company shall regularly perform risk monitoring by comparing the actual loss with the tolerance limit to promptly detect deficiencies in the policies, procedures and processes, and propose corrective actions. The frequency of monitoring shall be on a Monthly basis.

Key risk indicators shall be developed, to act as early warnings of increased in risk of potential losses. Effective tracking of these indicators by the Risk management & Compliance office shall allow the organisation to identify changing risks upon their occurrence and respond to them promptly.

C. Risk Assessment

Once risks are identified, they will be evaluated on a 2-dimensional matrix using a qualitative rating of the likelihood of the event occurring and the scale of the possible consequences. When risks have been identified, they are analyzed by combining the consequences and likelihood to produce a level of risk. This form of evaluation provides a good graphical representation of how serious the risk is or where it lies within a group of risks. The risk analysis provides information critical to determining what risks need to be treated and what risks are accepted.

The following matrices will be utilized for the assessment process:

Table 1 Consequence of Risk Event	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic
Actual / Potential Loss (The actual "gross" financial outflow as a consequence of a risk event, measured by % NOP or Premium Volume)	< 1%	1-3%	3-5%	5-10%	>10%
Reputational Impact (The potential consequence from a risk event note: the potential consequence may be any one of the two criteria)	No reputational** impact	Low reputational** impact	Medium reputational** impact.	High reputational** impact.	Significant risk to IndiaFirst and a partner reputation.
Legal (The potential consequential exposure to loss from legal action against IndiaFirst or a partner firm as a result of a risk event)			Any potential or threatened legal action, where we may need to reimburse the cost of litigation	Potential or threatened legal action with significant damages, adverse press or customer dissatisfaction leading to difficulty in marketing / distribution of company products	Potential or threatened legal action leading to class action lawsuit
Regulatory (The potential consequence of a risk event in respect of action by a regulator, Government Agency etc)	Regulatory interest very unlikely. No mitigating action will be required to reduce impact.	May lead to minor regulatory interest, capable of speedy resolution. Regulatory censure highly unlikely. Delays in reporting to the regulator.	Regulator will need to be advised and may require ongoing follow up of action taken. Capable of resolution within 1 year. Regulatory censure likely.	Regulator will be proactively involved in the event, requirement for proactive senior management involvement in resolution of issue with the regulator. Possible levying of penalties.	Event is of a nature that regulator might take enforcement action. Regulatory scrutiny likely to be intense. Potential temporary or permanent suspension of business operations.

Consequence Matrix

Risk events are given a severity score of between 1 and 5 based upon meeting one of the criteria within the categories of **Actual or Potential loss, Reputational Impact****, **Legal** and **Regulatory**. The severity score is determined by the highest of the 4 categories that the risk event triggers.

Reputational Impact (**)

The following factors should be used in determining the reputational impact of a risk event:

	Low	Medium	High	Significant
Media	No adverse comment is expected from the event. Knowledge of the event limited to the relevant business area.	Some limited adverse media comment could arise from the event.	Adverse comment in industry publications and / or national media anticipated. Proactive management of media required.	Considerable adverse comment across media sector anticipated. Considerable, high-level management focus will be required to mitigate the effects.
Customer	No customer complaints are anticipated from the event or its resolution.	Low levels of customer complaints are anticipated from the event or its resolution.	High Level of complaints may arise as a consequence of the event or its resolution.	Significant number of complaints may arise as a consequence of the event or its resolution. Event may result in withdrawal of business from the firm.
Employees	No or minimal impact on employee or employee relations	Event may result in contractual obligations to employees not being met	The event may result in adverse employee relations and poor employee morale and a potential for higher attrition rate	The event may result in industrial action, death or significant injury to employees

Table 2: Likelihood Matrix

Level	Descriptor	More Detail
A	Almost certain	Is expected to occur in most circumstances
B	Likely	The event will probably occur at least once
C	Possible	The event might occur at some time
D	Unlikely	The event is not expected to occur
E	Rare	The event may occur only in exceptional circumstances

Table 3: Level of Risk

Level of Risk (Heat Map)		Consequence				
Likelihood		1	2	3	4	5
		Insignificant	Minor	Moderate	Major	Catastrophic
	A	Low	Medium	High	Extreme	Extreme
	Almost Certain					
	B	Low	Medium	Medium	High	Extreme
	Highly Likely					
	C	Low	Medium	Medium	High	Extreme
	Likely					
	D	Low	Low	Medium	High	Extreme
	Less Likely					
	E	Low	Low	Low	Medium	High
	Rare					

Table 4: Risk Register

Compiled by:

Reviewed by:

Function/Activity:

Category	Risk What and how can it happen (Vulnerability)	Consequence	Likelihood	Existing Controls	Consequence Rating	Likelihood Rating	Level of Risk	Risk Priority
Fraud **(EXAMPLES ONLY)**	• Internal fraud • Employee collaborating with external party to launder money	• Financial loss to the company • Reputational damage	Possible	• Screening of staff at recruitment	4	C	High	2
Reputational	• Applications not reaching CPC • High CFR rate • Policy issuance % well below target	• Customer TAT unacceptable • Customer backlash • Impact on shareholders' business and reputation	Likely	• BDM training • "Verified & Ready for Login" stamps required	4	B	High	1

Last Board Approval Date: October 18, 2022