Fraud Risk Framework

Change History

Author	Reviewer/Approver	Version	Date of Release
Kapil Punwani	Kavita Maru	1.2	April - 2015
	Sunder Krishnan		
Kapil Punwani	Kavita Maru	1.3	April - 2017
	Sunder Krishnan		
Kapil Punwani	Kavita Maru	1.4	July 2018
	Sunder Krishnan		
Kapil Punwani	Kavita Maru	1.5	July 2019
	Sunder Krishnan		
Kapil Punwani	Kavita Maru	1.6	July 2020
	Sunder Krishnan		
Kapil Punwani	Kavita Maru	1.7	July 2021
	Sunder Krishnan		
Sukesh Sen	R Bharathwaj	1.8	July 2022
	Sunder Krishnan		
Sukesh Sen	R Bharathwaj	1.9	Oct 2022
	Sunder Krishnan		

Table of Content

4. **Roles & Responsibility**
5. **Awareness & Communication**
6. **Reference to Other Policies**
7. **Amendments and Reviews**
8. **Annexures & Templates**

1.Definition & Scope:

1.1 <u>Management Vision & Tone at the Top</u>: Fraud encompasses a range of irregularities and illegal acts by intentional deception or misrepresentation which an individual/organization/functions knows to be false.
Fraud Risk poses a significant impact to all departments/functions across the organization. Increase in fraud incidents reduces consumer and shareholder confidence and must have serious reputational, financial and regulatory impact.

As an organization Reliance Nippon Life Insurance (RNLIC) has zero tolerance towards all forms of frauds. It is therefore required that every employee understands the nature and impact of fraud to minimize the vulnerability of their day-to-day operations.

1.2 <u>Objective</u>:

The objective of Fraud Framework document is to define and provide guidance to identify, assess, respond, monitor, and report different types of Fraud Risks within RNLIC. This Framework is aligned to the overall Risk Management Strategy defined in the Enterprise Risk Management Framework of RNLIC.

This framework ensures that, the Management & employees understand the risk of fraud to the organization and establish a sound control environment through policies, procedures, and controls to detect, monitor and mitigate occurrences of frauds within various functions of the Organization that are vulnerable to the fraud risk.

This framework also helps to create awareness among all stakeholders including employees, clients and other parties having business relation with the Organization to deter them from indulging in fraudulent activities and measures to be taken by them in case they suspect any fraudulent activities.

<u>1.3 Scope:</u>

This policy applies to any fraud or suspected fraud involving vendors, customers, employees (all full time, part time or employees appointed on an ad-hoc / temporary /contract basis) and representatives of vendors, suppliers, contractors, service providers or any outside agencies doing any type of business with the Organization. This policy and framework apply to all employees across levels & positions.

For Agents, employees and intermediaries, the organization, upon identification and investigation of fraudulent events, Risk team must recommend actions to be taken on the perpetrators in consideration to the disciplinary action matrix.

This policy & Framework document also aims at:

- Driving the culture of ethics, honesty, understanding of Risk and controls
- Identify and assess possible fraud risks, develop, and implement processes & procedures to mitigate and reduce fraud opportunities
- Develop a process for fraud monitoring, mitigation, action to be taken and reporting
- Ensuring that the Management is aware of its responsibilities for developing and establishing processes and procedures to prevent or detect frauds when it occurs
- Providing guidance to employees, agents, intermediaries, customers, etc, to forbid them from getting involved in any fraudulent act and/ action to be taken by them when they suspect a fraud
- Provide a mechanism for the Organization employees to timely report or highlight a suspected or alleged fraud
- Provides guidance on how to conduct fair investigations and actions (internal and external) to be taken on completion of investigations.
- Providing assurance to all stake holders that all fraudulent activities/incidents will be investigated, dealt with, and not tolerated.

1.4 <u>Definition:</u>

a) Definition of Fraud: Fraud is generally defined as a deliberate misrepresentation to gain an advantage over a party. Fraud comes in many forms including fraud in Financial Statements, theft, disclosures, etc.
IRDAI has defined Fraud in insurance as an act or omission intended to gain dishonest or unlawful advantage for a party committing the fraud or for other related parties. This may, for example, be achieved by means of:

- Misappropriating assets.
- Deliberately misrepresenting, concealing, suppressing or not disclosing one or more material facts relevant to the financial decision, transaction or perception of the insurer's status
- Abusing responsibility, a position of trust or a fiduciary relationship

b) Attempted & Actual Fraud:

Attempted Fraud: An attempted fraud is an unsuccessful effort to commit the fraudulent act. This is when a fraudulent act has been identified before the Organization has any financial or non-financial impact. Generally, in such scenarios, the act of fraud could have been initiated. However, the internal controls help in preventing the financial/non-financial impact.

Actual Fraud: In order, for an act of fraud to be considered as actual, the act must be material, wilful and must have resulted in either a financial or non-financial impact to the other party. In such cases, the fraudulent act is successful in defrauding the customer and/or the organization and is generally detected after the fraud has been committed resulting in financial/non-financial loss to the customer and/or the Organization.

2. Fraud Classification –

To adequately protect itself from the financial and reputational risks posed by insurance frauds, RNLIC have in place this framework to protect the insurer from the threats posed by the following broad categories of frauds. SIRDAI XX some of the examples of fraudulent acts/omissions include, but are not limited to the following:

Policy holder Fraud-

Definition: Fraud against the insurer in the purchase and/or execution of an insurance product, including fraud at the time of making a claim

Examples:

a) Exaggerating damages/loss
b) Staging the occurrence of incidents
c) Reporting and claiming of fictitious damage/loss
d) medical claims fraud
e) Fraudulent Death Claims
f) Forgery

Internal Fraud-

Definition: Fraud/ misappropriation against the insurer by its Director, Manager and/or any other officer or staff member (by whatever name called).

Examples:

a) misappropriating funds
b) fraudulent financial reporting
c) stealing cheques
d) overriding decline decisions to open accounts for family and friends
e) inflating expenses claims/over billing
f) paying false (or inflated) invoices, either self-prepared or obtained through collusion with suppliers
g) permitting special prices or privileges to customers, or granting business to favoured suppliers, for kick backs/favours
h) forging signatures
i) removing money from customer accounts
j) falsifying documents
k) selling insurer's assets at below their true value in return for payment.
l) Forgery

Intermediary Fraud-

Definition: Fraud perpetuated by an insurance agent/Corporate Agent/intermediary/Third Party Administrators (TPAs) against the insurer and/or policyholders.

Examples:

a) Premium diversion-intermediary takes the premium from the purchaser and does not pass it to the insurer

b) Inflates the premium, passing on the correct amount to the insurer and keeping the difference

c) Non-disclosure or misrepresentation of the risk to reduce premiums

d) Commission fraud - Insuring non-existent policyholders while paying a first premium to the insurer, collecting commission and annulling the insurance by ceasing further premium payments.

e) Forgery

External/Third Party Fraud-

Definition: External or Third-party fraud is the risk of unexpected financial, material or reputational loss as the result of the fraudulent action of persons external to RNLIC.

Examples:

a) Hacking/Cyber crime
b) Theft of information
c) Theft of Organization assets
d) Vendor fraud
e) Loss of intellectual property

3. **Fraud Governance Structure:**

RNLIC encourages the culture of integrity, honesty, fairness, and high ethics to create a positive workplace environment for all employees. The Board of Directors and the Management sets the tone at the top for ethical behavior by communicating openly. The Code of Conduct is communicated to all employees and staff through trainings, HR Manual, Organization website, intranet, etc.

As part of an organization's fraud governance structure, a fraud risk management program includes are following but not limited to below:

3.1 Prevention & Detection

Fraud prevention is the implementation of a strategy to proactively identifying fraudulent transactions/actions and reduce the Impact/Likelihood of frauds by preventing these actions from causing financial and reputational damage to the organization. Detection process is used to detect frauds in any system or organization. The Organization must implement all possible measures of prevention techniques which includes but not limited to below:

- **Surveillance**: It refers to the proactive monitoring/observing suspicious activities and transactions through data analytics, continuous monitoring, and other available modes to identify probabilities of fraud. Data surveillance must analyze huge amounts of data, to identify patterns and reveal trends that must be used to mitigate fraud risk. Data Surveillance team would be the backbone of getting inputs from various sources and providing output on various alerts.

- ***Data Analytics:*** It refers to the process of examining data sets to increase efficiency and improve performance by discovering patterns & drawing conclusions based on data. Fraud risk team must use various tools and techniques to perform data analytics on fraud risk scenarios based on new emerging trends, identified scenario-based testing, smart sampling and validation of data/documents.

- ***Training & Awareness:*** To embed risk culture in organization, the Fraud risk team must create fraud risk awareness through training and communication to its employees, intermediaries & vendors. Attention to be paid to the employees working in high-risk profiles/process to mitigate fraud risk. The Organization must also educate its customers well about fraud awareness and solicit their participation in various preventive / detective measures

- ***Signoff for New Process/*** **Modification in existing processes*:*** New processes and existing process changes from the various functions must be reviewed by Fraud risk team for sign off before rolling out as a communication. This enables Fraud risk team to identify loopholes if any at the initial stage.

- ***Employment Screening:*** It is a process in which the organization verifies candidate's background to assess their previous employment and criminal history. The organization will have documented policies and procedures in place to exclude any unsuitable employee and increases the effectiveness of the employment process.

- **Pre issuance verification:** As part of the various prevention and detection strategies, the Organization must develop methodologies to curtail or restrict addition of fraudulent/non-insurable/sub-standard profiles before the issuance of the policies on sampling basis.

- **Post Issuance Verification:** The Organization must also develop procedures to identify and investigate cases, that are not investigated prior to issuance policies (PIRV).

- **Mystery Shopping** - Mystery shopping must be used to measure quality of service, job performance, regulatory compliance, or to gather specific information about a vendor, market, or competitors.

- **Continuous Monitoring** – It is an activity of regularly identifying and assessing potential fraud risks through monitoring of emerging trends, incidents, red flags & early warnings which enables the management to gather data, testing risk scenarios & review business processes for adherence to and deviations from their desired performance and effectiveness.

- **Forensic Investigations:** Forensic investigative services and fraud risk management help in preservation of a company's reputation and tangible and intangible assets. Clarifying any discovered inconsistencies, investigating cases of fraud and corruption, settling arguments, dealing with issues related to inspection institution oversight, and responding

quickly to cybercrime threats are all components of a fool proof system to stop fraud and ensure a business' security.

By highlighting common flaws in an infrastructure, application, or website, forensic analysis techniques provide valuable information. Security software can prioritise fixing these vulnerable areas based on this information.

Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court. Cyber forensics is also known as computer forensics. Electronic equipment stores massive amounts of data that a normal person fails to see.

The main aim of cyber forensics is to maintain the thread of evidence and documentation to find out who did the crime digitally. Cyber forensics can help in:

- Recover deleted files, chat logs, emails, etc
- Recover deleted SMS, Phone calls.
- Extract recorded audio of phone conversations
- Determine which user used which system and for how much time.
- Identify which user ran which program

Cyber forensic may use below indicated methods to investigate a fraud:

- Network forensics: This involves monitoring and analyzing the network traffic to and from the perpetrators network. The tools used here are network intrusion detection systems and other automated tools.
- Email forensics: In this type of forensics, the experts check the email of the perpetrators and recover deleted email threads to extract out crucial information related to the case.
- Malware forensics: This branch of forensics involves hacking related crimes. Here, the forensics expert examines the malware, trojans to identify the hacker involved behind this.
- Memory forensics: This branch of forensics deals with collecting data from the memory (like cache, RAM, etc.) in raw and then retrieve information from that data.
- Mobile Phone forensics: This branch of forensics generally deals with mobile phones. They examine and analyze data from the mobile phone.
- Database forensics: This branch of forensics examines and analyzes the data from databases and their related metadata.
- Disk forensics: This branch of forensics extracts data from storage media by searching modified, active, or deleted files.

- **Surprise Branch Review -** A surprise branch review is to assess the functioning of the set processes & branch activities to ensure Organization's internal controls are effective. It is intended to prevent and detect fraud as it minimises the opportunity/scope to prepare for the audit in advance.

- **Financial Reconciliation -** Financial reconciliation is an accounting process that compares two or more sets of data records to verify that figures are correct and balanced. Periodic financial reconciliation must confirm that accounts in the financial books are consistent, accurate, and complete.

- **Whistle blower:** Whistle blowing is an effective tool to perceive fraud, wrongdoing, misconduct, unethical practices within or outside of the organisation. A strong culture of whistleblowing helps to identify all manner of potential risks, financial losses and process breaches by taking the action & strengthening the controls

3.2 Cyber Fraud:

Financial transactions executed through use of a fake or stolen debit/credit card or bank account to make a payment on the Organization portal or website. Cyber fraud also includes Compromise of Organization data or customer information due to a cyber-attack or hacking of Organization computer systems.
The Organization must have well defined procedures to identify, detect, prevent, investigate and report Information Security frauds and violations. The Risk Management and Information security function must develop and manage systems, processes and framework with analytical tools methodologies to identify potential fraud areas or red flags.

Through risk-based sampling methodology, the Risk & Information security team will identify patterns/ events to review processes and will put in place preventive measures and subsequently report to the Risk Control Committee, which oversees Fraud Monitoring functions.

The Risk Management & Information security function also delivers Cybersecurity awareness trainings regarding trending risks and for frauds prevention across the Organization to develop a culture of zero tolerance to Security violation and frauds.

The organization must establish a Cyber fraud cell to address and mitigate the cyber-crimes like hacking, ransomware, data theft, hoax calls, identity theft, phishing etc.

RNLIC must share reported hoax call contact numbers to Telecom Regulatory Authority of India (TRAI) on monthly basis.

Confidentiality

All fraud investigations and related information must be treated confidentially. Investigation matters and results will not be disclosed or discussed with anyone other than those who have valid business need to know.

Disciplinary Measures

Based on investigation findings, the accountability, and complicit disciplinary measures must be decided. Efforts must be made to recover the loss amount fully. Based on the nature of violation or fraud, an internal committee may decide on suitable penal action as per the action matrix or pursue the matter with other law enforcement agencies for appropriate action against the concerned.

Exchange of Information

The Organization may exchange requisite information on Information security violations or frauds with other insurers through Life Council, IIB or Authority as and when required. The Organization must aid in setting up coordination platforms through Life Council or any other Forum to establish information sharing mechanisms.

3.3 Fraud Risk Assessment

The Fraud Risk Team has the primary responsibility of establishing and monitoring all aspects of fraud risk assessment and prevention activities. The fraud risk assessment must identify potential fraud risk areas and the perpetrators. The assessment must be commensurate with the business size of the Organization. Fraud Risk Team must establish policies and procedures to:

- Identify and assess frauds
- Set up procedures to mitigate the identified fraud risks
- Implement preventive and detective measures through internal controls
- Liaising with law enforcement agencies

The Fraud risk assessment must include fraud risk identification, likelihood, significance, and response. The fraud risk assessment must be performed at all possible levels (Entity/ function/process/location). This must be documented, reviewed, and updated as required or at least once annually to identify potential fraud events and consider mitigation plans. Fraud risk assessments are also done through RCSA (Risk Control Self Assessment) where the controls are tested as per defined frequency depending on the criticality of the risks. Fraud risk related findings/observations of any audit will also be considered while conducting assessments of various fraud risks.

3.4 Investigation & Response Plan

Response plans are the steps & actions taken by the organization in dealing with a potential fraudulent incident. An effective response plan has four steps as below:

1. **Alert Generation**
2. **Investigation**
3. **Report Creation**
4. **Follow-up Actions**

Alert Generation: Potential list of incident/complaints (indicative) received from various entities included below:

Themes	Trigger/Source	Understanding
Policy Lifecycle	CMU	Received from Complaint Management Unit
Whistle Blower	Whistle Blower	Received directly from some unknown source, where source is not identifiable from mail content as well to whistleblower / rlife.ombudsman id
Policy Lifecycle	PIRV	Post Issuance Risk Verification
Policy Lifecycle	Pre-issuance/UW	Received from Underwriting
Policy Lifecycle	Escalated Complaints-Received from CEO/CXOs/HODs/Group	This would include any case forwarded to you which has a initial mail where a customer has raised his concern at source
Policy Lifecycle	Escalated Case - Received from CEO/CXOs/HODs/Group	This would include any case forwarded to you which has a initial mail where an unknown person has raised some whistle blower
Policy Lifecycle	Branch-Complaint	This would have cases where branch has forwarded complaints received at branch. Technically these nos. should be less or negligible as they are supposed to raise the complaint in CRM routed through CMU
Whistle Blower	Branch-whistle-blower	This would have cases where branch (Sales/ non-Sales) has raised a Whistle blower
Policy Lifecycle	Claim	As is, mostly includes CRC cases
Data Analytics	Risk Review / Self investigation	Cases picked up through self-data analysis and not received from any other employee
Other Function	Finance, Audit, IT, Admin & Investment	Received from other functions
Policy Lifecycle	Legal / Ombudsman	Legal/Ombudsman cases for investigation
Policy Lifecycle	Social Media	Customer complaints escalated on social media

Investigations: The purpose of an investigation is to establish relevant facts to prove or disprove allegations of fraud. It is a fact-finding process conducted in an impartial and objective manner, with the aim to establish the relevant facts and initiate necessary changes to system/process & controls to mitigate risks.

The fraud investigation must consist of gathering sufficient information about specific details and performing those procedures that are necessary to determine whether fraud has occurred, the loss or exposures associated with the fraud, who was involved in it and the fraud scheme (how it happened).

The Organization would design policies, framework, and procedures to investigate various types of fraud allegations that may have been reported & identified through various sources. The Fraud Risk Team will ensure that the investigations are conducted in an impartial manner. The Fraud Risk Team is authorized to take into custody of all relevant records, documents, and other evidence related to the relevant investigation to protect them from being stolen, tampered, destroyed or removed by the suspected perpetrators. The full records of the investigation, including interview notes, must be kept under secured access with investigator till the completion of the investigation.

The investigations must be kept as confidential and private as possible to ensure the least amount of disruption to the Organization and always maintain the process integrity. Confidential information will be shared only on a "need-to-know" basis with required approval.

Once investigations are complete and risk findings are identified, thereafter the Fraud Risk Team team must initiate and take necessary actions including but not limited to approaching Law Enforcement Agencies after approval from competent authority whenever appropriate

Report Creation: A fraud investigation report is required to get an understanding of the fraud investigator's specific activities, findings, conclusion, and recommendations. Report creation is necessary to determine further appropriate course of action by the authorities within the organization. The Fraud Investigator is responsible for providing accurate and unbiased reports depicting the investigation results clearly.

The conclusion and results of the investigations must be duly documented in writing. The report gives narration of the issue reported, steps taken and investigation findings along with available evidence. The report must contain at least following sections: -

1. **Background: -** A brief description of allegation/information and source of information.
2. **Scope: -**This section of report shall contain the subject of investigation.
3. **Approach: -**This section shall contain the process of investigation in brief about obtaining information, reviewing, and analyzing data/documents, use of surveillance and list of individuals interviewed.
4. **Findings: -** This section shall contain the chronology of events, evidence, information procured and examiner's findings.
5. **Executive Summary: -** This section of report shall include summary of the case with findings and conclusion.
6. **Impact on organization: -** This section shall describe the impact of fraud on Organization i.e., Financial, reputational, operational risk etc.
7. **Root Cause Analysis: -** This section shall focus on gaps and failures.
8. **Recommendation:** - This section shall define the action to be taken based on the evidence and findings.

Owner of Report: - Fraud investigator shall be responsible for preparing and owning the fraud examination report.

Repository: - Physical/original Investigation report shall store with the Centralized repository for future requirement.

Inputs to Analytics Team: Share the investigation and RCA findings with Analytics team to do further analysis and do proactive identification of any such fraud trends.

Process Improvements: Suggest Process Improvement, which is proactive task of identifying, analyzing, and improving upon existing business processes within organization for optimization and to meet standards of quality.

Corrective/ Follow-up Actions:

Investigation: Below actions must be taken to respond to any alleged or suspected incident of fraud

- Conduct detailed investigation of the incident
- Obtain/procure evidence and information
- Penal actions to be taken as per predefined matrix
- Relevant gaps and controls be assessed for improvement

Corrective actions:

Disciplinary Action: A consistent and credible disciplinary system is a key control for deterring fraud. At RNLIC, we have a well-defined disciplinary actions procedure & accountability matrix to fix accountability and consequences on the perpetrators

Legal Action/Recoveries: Post investigation based on evidence if it has been proven that there is financial/reputational loss to RNLIC, then corrective actions must be taken for recovery from fraudster and if required legal action would be initiated post obtaining necessary approvals.

Financial fraud Loss, recovery and compensation: Fraud risk team must prepare a process note covering treatment in the books of account for financial loss and recoveries identified from fraud/operational loss events. This must provide guidelines for the functions for booking of loss, recoveries, settlement, creating provisions, required approvals, etc. in coordination with Finance team.

In all cases wherein the financial fraud is established & it is proven that the policyholder has been defrauded by the fraudsters and RNLIC is liable to pay to the customers, such cases need to be taken forward to compensate the impacted policyholders.

The Organization must have a process note in place with documented authority matrix to approve & pay the impacted customer irrespective of fraud loss recoveries.

3.5 – Governance & Reporting

Governance:
IRDAI Corporate Governance guidelines for Insurance Companies require set up of a mandatory Risk Management Committee (RMC). Fraud Risk governance includes mechanism that ensures accountability and authority for the management of risks, implementation, and continuous improvement of Risk Management framework; and provides Risk Management assurance.

We have below Governance structure for reporting & monitoring of frauds in the organization:

1. **Zonal Ethics & Disciplinary Committee –** It comprises of Zonal Risk manager, Zonal HR manager, Zonal operations Manager, Zonal managers (sales & distribution) & Zonal Fraud control manager (FRAUD RISK TEAM). ZEDC is conducted monthly and reviews the investigated cases and recommends the actions to CEDC.

2. **Central Ethics & Disciplinary Committee -** It comprises of CHRO, Chief Distribution Officer, Head of Risk, Head of Operations, AVP- Risk and HR National Manager-Employee Relations. CEDC reviews the recommendations of ZEDC and takes the final decision. Frequency – Once a month/as required.
3. **Control Committee –** Headed by CEO, participated by CXO's, CRO, Head of Risk and other participants as per requirement. Identified Frauds and actions taken must be reported in this committee on monthly basis.
4. **Board Risk Management Committee –** It comprises of the Board of Directors of the Organization and committee meetings are conducted quarterly. BRMC is responsible for providing directions and monitoring of risk and mitigation at the organization level.

Reporting

Internal Reporting

Fraud and violations must be reported and presented to the relevant Committees held periodically. The report detail statistics of fraud cases, summary on key cases identified, Loss amounts, resolution, and actions etc.

External Reporting

The Organization submits Annual report on fraud cases to IRDAI in forms FMR-1 and FMR-2 as required by the Regulator to provide details of outstanding & closed cases. For reporting under FMR, cases that have been reported for investigation, must be considered as closed/open based on status of investigation internally or externally with Law enforcement agencies.

Records Retention

All information security violations and fraud related data/ documents must be preserved for a period as specified in the applicable regulations. These should be presented when asked by Authorities during periodic Audits/ Inspections.

Root cause analysis is a systematic process with conclusions backed up by evidence for identifying "root causes" of problems or events. The RCA may also provide an approach for responding to them. Root cause analysis must include the "cause and effect" statements. It uncovers the fundamental causes of problems such as fraud.

The main objective of the fraud investigation is 'WHY' the event occurred, and not who made the error. An RCA report must include a risk mitigation plan. RCA explains about identified risks during investigation and recommends solutions.

4. Roles & Responsibilities –

Board of Directors- The Board of Directors oversees that Senior Management lays down and implements the Fraud Risk Management Policy.

Board Risk Management Committee (BRMC): RNLIC has Risk Management Committee of Board that meets every quarter. Critical fraud risk cases are reviewed by BRMC every quarter. The BRMC provides guidance and directions to the Risk for corrective measures to be adopted and process improvements.

Chief Risk Officer- Chief Risk Officer is entrusted with the responsibility to ensure that the monitoring of the Fraud and forgery cases across the organization and report their progress Audit/Risk Committee and the Board at a Quarterly frequency. It is the responsibility of the Chief Risk Officer to ensure that the responsible functions are aware of their duties and responsibilities in identification, monitoring, and reporting of fraud along with procedure for Governance Action.

Legal & Compliance - This function co-ordinate with law enforcement agencies, for reporting frauds on timely and expeditious basis and follow-up processes thereon. It is the responsibility of Legal & Compliance function to do all the required regulatory reporting and inform service providers / vendors / third parties / customers (existing and new both) about the anti-fraud policy of the Organization and consequences of submitting a false statement and/or incomplete statement.

Risk Management – It must assist in identifying and assessing fraud risks and help management to design specific controls to mitigate fraud risks. In addition, by carrying out fraud risk assessments, this team must proactively detect indications of fraud in those processes or transactions where analysis indicates the risk of fraud to be significant or high. Risk function also need to ensure the effective communication and awareness about fraud risk within the organisation. Risk function must have disciplinary action matrix in place to take actions on agents/intermediaries for malpractices if proven.

Human Resource – Human Resource function must have policies and procedures to ensure verification of pre-employment history of the prospect employees. HR must also have a disciplinary action matrix in place which is to be followed to take actions on employees for malpractices if proven.

Internal Audit - It must assist in the deterrence of fraud by examining and evaluating the adequacy and the effectiveness of the system of internal controls and by conducting proactive auditing to search for fraud. Internal Audit may support and cooperate with the Fraud Investigation Team, gathering information and making recommendations.

Audit Committee - The Audit Committee must also ensure that senior management implements appropriate fraud deterrence and prevention measures. The Audit Committee must receive periodic reports describing the nature, status and disposition of any fraud or unethical conduct.

Employees and officers at every level, in every function, at all offices of the Organization and at all the locations have a responsibility to speak up when they believe that they have knowledge or suspect that fraud is being committed. As soon as it is learnt that a fraud or suspected fraud has taken or is likely to take place, they should immediately apprise the same to the concerned party as per the laid down procedures in place.

Information technology – It is the use of any computers, storage, networking and other physical devices, infrastructure, and processes to create, process, store, secure and exchange all forms of electronic data. IT helps in securing the information with the help of firewalls, encryption and DLP tool.

5. Culture Building – Anti Fraud Risk

Culture is frequently regarded as a factor that produces specific types of organisational control based on shared values and beliefs. In other words, when employees within a company share a common organisational culture framework, they behave in ways that benefit the company financially as well as in terms of risk assessment.

Training/Awareness: To embed risk culture in organization, the Fraud risk team must conduct fraud risk awareness through training and communication to its employees, intermediaries, vendors, and customers. Attention to be paid to the employees working in high-risk profiles/process to mitigate fraud risk. The Organization will also educate its customers as well about fraud awareness part of various preventive measures

1. Fraud risk awareness session must be included in new employee induction program.

2. E-learning modules must be introduced to educate the employee on potential fraud risks.

3. Publishing the newsletters, risk advisories, and case studies to embed fraud risk culture.

4. Fraud awareness communication to customers/public on Organization's website/social media platforms to create awareness.
5. Promoting whistle-blow culture.

6. Reference to Other Policies:

-Whistleblower Policy
-Employee Code of Conduct
-Cyber Risk
-InfoSec Policy
-Contracts/Agreements (Agent/Intermediary/Vendor)
- HR policies

7. Annexures & Templates

-Malpractice Action Matrix
-Root Cause Analysis
-Investigation Report

-FMR
Fraud Risk Dashboard(FCU team to share)

8. Amendments and Review

Risk Management Committee is authorized to make amendments to this Policy at any time, when considered appropriate to do so, within the overall framework stipulated by IRDAI. The amendments
approved by the Risk Management Committee must be put up to the Board, at its next meeting, for
ratification.

Annexures & Templates

1. Malpractice Action Matrix

RELIANCE NIPPON LIFE INSURANCE

Action Matrix- Responsibility flowover concept.

Risk cases		First Level of Sourcing				Second Level of Sourcing				Third Level of Sourcing				Fourth Level of Sourcing			
Risk cases	Sub Category	Further Investigation	1st Instance	2nd Instance	3rd Intance	Further Investigation	1st Instance	2nd Instance	3rd Intance	Condition (time span: 6 months)	1st instance (2SMs)	2nd Instance (4SMs)	3rd Intance (6SMs)	Condition (time span: 1 year)	1st instance (4SMs)	2nd Instance (8SMs)	3rd Intance (10SMs)
Death Claim	Fraud Claim due to age proof tampering	Huge age difference (> 7 years)	Termination			Huge age difference (> 7 years)	Warning	Warning + Demotion	Termination	2 or more SMs/ 2 instances	Warning	Termination		2 or more TM's/ 4 instances	Warning	Termination	-
		Minimal age difference (3 to 7 years)	Caution	Warning	Termination	Minimal age difference (3 to 7 years)	Caution	Warning	Termination	2 or more SMs/ 2 instances	Caution	Warning	Termination	2 or more TM's/ 4 instances	Caution	Warning	Termination
	Insuring a dead person	Prior to March 2013	Termination			Prior March 2013	Warning	Termination									
		Post March 2013	Termination			Post March 2013	Termination			2 or more SMs/ 2 instances	Warning	Termination	-	2 or more TM's/ 4 instances	Warning	-	-
	Any terminal/ pre-existing disease which is apparent		Termination				Warning	Warning + Demotion	Termination	2 or more SMs/ 2 instances	Warning	Termination	-	2 or more TM's/ 4 instances	Warning	-	-
	Any terminal/ pre-existing disease which is not apparent and policy holder is related		Termination				Warning	Warning + Demotion	Termination	2 or more SMs/ 2 instances	Warning	Termination	-	2 or more TM's/ 4 instances	Warning	-	-
	Early death claims	2 death claims repudiated in a span of 12 months	Termination			4 death claims repudiated in a span of 12 months	Warning + Demotion	Termination		2 or more SMs/ 2 instances	Warning			2 or more TM's/ 4 instances	Caution		
	Any terminal/ pre-existing disease which is not apparent and policy holder is not related	-	Caution	Warning	Termination	-	Caution	Warning	Termination		Caution	Warning	Termination	2 or more TM's/ 4 instances	Caution	-	-
Malpractice complaints	Signature, Medicals, Proposal form, Documents submitted by client	No Financial impact	Warning	Termination		No Financial impact	Caution	Warning	Termination	2 or more SMs/ 2 instances	Caution	Warning	Termination	2 or more TM's/ 4 instances	Caution	-	-
		Financial impact	Termination			Financial impact	Warning	Warning + Demotion	Termination	2 or more SMs/ 2 instances	Warning	Termination	-	2 or more TM's/ 4 instances	Warning	-	-
	Illegal method of business	No Financial impact	Caution	Warning	Termination	No Financial impact	Caution	Warning	Termination	2 or more SMs/ 2 instances	Warning	Termination	-	2 or more TM's/ 4 instances	Warning	-	-
		Financial impact	Termination			Financial impact	Warning	Warning + Demotion	Termination	2 or more SMs/ 2 instances	Warning	Termination	-	2 or more TM's/ 4 instances	Warning	-	-
Submission of Fake documents	Documents submitted are forged/fake		Termination		-	Financial impact	Warning	Warning + Demotion	Termination	2 or more SMs/ 2 instances	Warning	Termination	-	2 or more TM's/ 4 instances	Warning	-	-
Conflict of Interest	Undisclosed relationship	No Financial gain/performance	Deconflict & Warning	Termination	-	No Financial gain/performance	Deconflict & Warning	Termination	-	2 or more SMs/ 2 instances	Warning	Termination	-	2 or more TM's/ 4 instances	Caution	-	-
		Financial gain	Termination		-	Financial gain	Termination		-	2 or more SMs/ 2 instances	Termination	-	-	2 or more TM's/ 4 instances	Warning	-	-
Infosec Violation	DLP Incident - Sharing of confidential data through mail or external device	Confidential information / critical to company	Caution	Warning	Termination	Confidential information / critical to company	Caution	Warning	Termination	2 or more SMs/ 2 instances	Caution	Warning	Termination	2 or more TM's/ 4 instances	Caution	-	-
		Others	Advisory			Others	Advisory										
Mis-selling	Wrong Promises made to Client / Charges & return related	Based on impact	Warning	Termination	-	Based on impact	Caution	Warning	Termination	2 or more SMs/ 2 instances	Caution	Warning	Termination	2 or more TM's/ 4 instances	Caution	Warning	Termination
Please note the following:-																	
*For anyone with vintage > 3 years, the action will be one level below for all cases - Except for deadman insurance cases post March 2013																	
For Deadman insurance cases post March 2013 and the vintage > 3 years **(1st instance)** - the Overall business, persistency and no of claims will decide the action as per the matrix or one level below																	

2. **RCA Template**

5 WHYs ROOT CAUSE ANALYSIS TEMPLATE	
Incident / Event	
Frequency of Incident / Event	New / Repeat
Severity of the Incident / Event	Red/ Amber/ Green
Risk Score	Very High/ High/ Moderate/ Low
Impact Financial / Regulatory etc	
Functions Accountable	
Date Action Begin	
Date Action Close	
DEFINE THE PROBLEM	It is happening because (Define Problem Here)
WHY IS THIS A PROBLEM?	**PRIMARY CAUSE**
	1.Why is it happening?
	It is happening because
	2.Why is that?
	It is happening because
	3.Why is that?
	It is happening because
	4.Why is that?
	It is happening because
	ROOT CAUSE
	5.Why is that? (NOTE: If the final "Why" has no controllable solution, return to the previous "Why.")
	It is happening because (ROOT CAUSE)
CORRECTIVE ACTION TO TAKE	Describe action here

Investigation Template

Internal Investigation Report

- **Source of Complaint (Channel- Branch/ Whistleblower) :-**
- **Mode of Complaints (Letter/ E-Mail/ On-Call/ Walk-in):-**
- **Repeat Complaint (If Yes, then earlier Unique ID): -**
- **Type of Fraud (Policy Holder/Intermediary/External/Internal/Third Party) :-**

- **Complainant Details:-**

Policy No/Vendor Name	Name	Address	Contact No	Location	State

- **Complaint Details:**

Complaint summary:

Policy Number	
Proposer/Life Assured Name	
Policy Issuance Date	
Risk Commencement Date	
Sum Assured	
Annual Premium	
Premium Mode	
Incident Date	
Complaint Receive Date	
Complainant Email ID	
Complainant Address	
ID Proof Collected	

- **Start Date of Investigation:-**
- **Chronology of Events:-**
- **Investigation Findings:-**
- **Date of Investigation Report Submitted:-**
- **Investigation Period (No of days taken to complete the Investigation):**
- **Evidences Procured:-**
- **Root Cause Analysis (RCA)/ Key Findings:-**
- **Scope for Process Improvement:-**

- **Legal action Required:-**

- **Recovery (if any):-**

- **Investigation Recommendation:-**

- **Input to Data Analytics:-**

- **Enclosures/Supporting**

Investigator Sign and Stamp

Name:-
Date:-
Place:-

FMR Template

RELIANCE NIPPON LIFE INSURANCE
A RELIANCE CAPITAL COMPANY

FRAUD MONITORING REPORT FOR THE YEAR 2020-21

FMR-I

PART-I

Frauds Outstanding Business segment wise

1. Non Linked

1.1 Non Linked- Participating

S.No	Description of Fraud	Unresolved cases at the beginning of the year		New cases detected during the year		Cases closed during the year		Unresolved cases at the end of the year	
		No.	Amount involved (in Rs. Lakhs)	No.	Amount involved (in Rs. Lakhs)	No.	Amount involved (in Rs. Lakhs)	No.	Amount involved (in Rs. Lakhs)
A	**Policyholder Fraud**								
	Falsifying documents	0	0.00	0	0.00	0	0.00	0	0.00
	Cash Frauds	0	0.00	0	0.00	0	0.00	0	0.00
	Fradulent claims	0	0.00	0	0.00	0	0.00	0	0.00
	Misselling/Signature Forgery	0	0.00	0	0.00	0	0.00	0	0.00
	Fradulent loan/surrender	0	0.00	0	0.00	0	0.00	0	0.00
	Benami Agency	0	0.00	0	0.00	0	0.00	0	0.00
	Reporting and claiming of fictitious damage/loss	0	0.00	0	0.00	0	0.00	0	0.00
	Wrong NEFT payments	0	0.00	0	0.00	0	0.00	0	0.00
	Sub Total (A)	**0**	**0.00**	**0**	**0.00**	**0**	**0.00**	**0**	**0.00**
B	**Intermediary Fraud**								
	Misappropriation of Funds	0	0.00	0	0.00	0	0.00	0	0.00
	Fradulent claims	0	0.00	0	0.00	0	0.00	0	0.00
	Misselling/Signature Forgery	0	0.00	0	0.00	0	0.00	0	0.00
	Impersonation/Identity Theft/Non-existent entity	0	0.00	0	0.00	0	0.00	0	0.00
	Fake receipts / Forged Documents	0	0.00	0	0.00	0	0.00	0	0.00
	Intermediary Fraud (Non-disclosure or misrepresentation of the risk to reduce premiums)	0	0.00	0	0.00	0	0.00	0	0.00
	Commission fraud	0	0.00	0	0.00	0	0.00	0	0.00
	Misappropriation of policy holders money by taking loans and surrenders	0	0.00	0	0.00	0	0.00	0	0.00
	Diversion of customers prem / claim to 3rd party	0	0.00	0	0.00	0	0.00	0	0.00
	Fraudulent loan/surrender	0	0.00	0	0.00	0	0.00	0	0.00
	Misuse of premium amount by Empowered Agent	0	0.00	0	0.00	0	0.00	0	0.00
	Sub Total (B)	**0**	**0**	**0**	**0.00**	**0**	**0.00**	**0**	**0.00**

S.No	Description of Fraud	Unresolved cases at the beginning of the year		New cases detected during the year		Cases closed during the year		Unresolved cases at the end of the year	
		No.	Amount involved (in Rs. Lakhs)	No.	Amount involved (in Rs. Lakhs)	No.	Amount involved (in Rs. Lakhs)	No.	Amount involved (in Rs. Lakhs)
C	**Internal Fraud**								
	Claim Related Fraud & Forgery	0	0.00	0	0.00	0	0.00	0	0.00
	Misselling/Signature Forgery	0	0.00	0	0.00	0	0.00	0	0.00
	Fraudulent loan/surrender	0	0.00	0	0.00	0	0.00	0	0.00
	Forged Documents	0	0.00	0	0.00	0	0.00	0	0.00
	Misappropriation of Funds	0	0.00	0	0.00	0	0.00	0	0.00
	Non Disclsoure	0	0.00	0	0.00	0	0.00	0	0.00
	Impersonation/Identity Theft/Non-existent entity	0	0.00	0	0.00	0	0.00	0	0.00
	False Invoices	0	0.00	0	0.00	0	0.00	0	0.00
	Fraudulent encashment of cheques	0	0.00	0	0.00	0	0.00	0	0.00
	Payment out of income heads	0	0.00	0	0.00	0	0.00	0	0.00
	Permitting special prices to suppliers	0	0.00	0	0.00	0	0.00	0	0.00
	Falsifying documents	0	0.00	0	0.00	0	0.00	0	0.00
	Stealing Cheques	0	0.00	0	0.00	0	0.00	0	0.00
	Registration and completion of New business without complying for basic mandatory documents	0	0.00	0	0.00	0	0.00	0	0.00
	Double Neft payment of PH NEFT Batch dated 28.08.2018	0	0.00	0	0.00	0	0.00	0	0.00
	Sub Total (C)	**0**	**0**	**0**	**0.00**	**0**	**0.00**	**0**	**0.00**
D	**Sub Total (A+B+C)**	**0**	**0**	**0**	**0.00**	**0**	**0.00**	**0**	**0**

1.2 Non Linked- Non Participating

S.No	Description of Fraud	Unresolved cases at the beginning of the year		New cases detected during the year		Cases closed during the year		Unresolved cases at the end of the year	
		No.	Amount involved (in Rs. Lakhs)	No.	Amount involved (in Rs. Lakhs)	No.	Amount involved (in Rs. Lakhs)	No.	Amount involved (in Rs. Lakhs)
E.	Policyholders Fraud								
	Cash Frauds	0	0.00	0	0.00	0	0.00	0	0.00
	Fradulent claims	0	0.00	0	0.00	0	0.00	0	0.00
	Misselling/Signature Forgery	0	0.00	0	0.00	0	0.00	0	0.00
	Non Disclsoure	0	0.00	0	0.00	0	0.00	0	0.00
	Falsifying documents	0	0.00	0	0.00	0	0.00	0	0.00
	Fradulent loan/surrender	0	0.00	0	0.00	0	0.00	0	0.00
	Benami Agency	0	0.00	0	0.00	0	0.00	0	0.00
	Reporting and claiming of fictitious damage/loss	0	0.00	0	0.00	0	0.00	0	0.00
	Wrong NEFT payments	0	0.00	0	0.00	0	0.00	0	0.00
F.	Intermediary Fraud								
	Misappropriation of Funds	0	0.00	0	0.00	0	0.00	0	0.00
	Fradulent claims	0	0.00	0	0.00	0	0.00	0	0.00
	Misselling/Signature Forgery	0	0.00	0	0.00	0	0.00	0	0.00
	Intermediary Fraud (Non-disclosure or misrepresentation of the risk to reduce premiums)	0	0.00	0	0.00	0	0.00	0	0.00
	Fake receipts / Forged Documents	0	0.00	0	0.00	0	0.00	0	0.00
	Fraudulent loan/surrender	0	0.00	0	0.00	0	0.00	0	0.00
	Impersonation/Identity Theft/Non-existent entity	0	0.00	0	0.00	0	0.00	0	0.00
	Misappropriation of policy holders money by taking loans and surrenders	0	0.00	0	0.00	0	0.00	0	0.00
	Diversion of customers prem / claim to 3rd party	0	0.00	0	0.00	0	0.00	0	0.00
	Cash stolen from safe	0	0.00	0	0.00	0	0.00	0	0.00
	Misuse of premium amount by Empowered Agent	0	0.00	0	0.00	0	0.00	0	0.00
	Sub Total (F)	**0**	**0.00**	**0**	**0.00**	**0**	**0.00**	**0**	**0.00**
G	Internal Fraud								
	Misappropriation of Funds	0	0.00	0	0.00	0	0.00	0	0.00
	Claim Related Fraud & Forgery	0	0.00	0	0.00	0	0.00	0	0.00
	Misselling/Signature Forgery	0	0.00	0	0.00	0	0.00	0	0.00
	Non Disclsoure	0	0.00	0	0.00	0	0.00	0	0.00
	Forged Documents	0	0.00	0	0.00	0	0.00	0	0.00