IndusInd Nippon Life Insurance Company Limited

Fraud Risk Framework
Version 2.3

IndusInd Nippon Life

Change History

Author	Reviewer/Approver	Version	Date of Release
Kapil Punwani	Kavita Maru Sunder Krishnan	1.2	April 2015
Kapil Punwani	Kavita Maru Sunder Krishnan	1.3	April 2017
Kapil Punwani	Kavita Maru Sunder Krishnan	1.4	July 2018
Kapil Punwani	Kavita Maru Sunder Krishnan	1.5	July 2019
Kapil Punwani	Kavita Maru Sunder Krishnan	1.6	July 2020
Kapil Punwani	Kavita Maru Sunder Krishnan	1.7	July 2021
Sukesh Sen	R Bharathwaj Sunder Krishnan	1.8	July 2022
Sukesh Sen	R Bharathwaj Sunder Krishnan	1.9	Oct 2022
Arni Shah	R Bharathwaj Sunder Krishnan	2.0	Oct 2023
Karanpreet Kaur	Kishor Panchal R Bharathwaj	2.1	Oct 2024
Shilpa Arora	Kishor & Vijay R Bharathwaj	2.2	Oct 2025
Shilpa Arora	Kishor & Vijay Arni Shah	2.3	Jan 2026

IndusInd Nippon Life

Table of Contents

1. Definition & Scope:

1.1. Management Vision & Mission at the Top:

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 IndusInd Nippon Life Insurance (INLIC) 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. Objective:

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 INLIC. This Framework is aligned to the overall Risk Management Strategy defined in the Enterprise Risk Management Framework of INLIC.

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.

1.3. Scope:

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. Definition:

a) **Insurance Fraud:**

Fraud in insurance is an act or omission intended to gain advantage through dishonest or unlawful means, for a party committing the fraud or for other related parties; including but not limited to:

- Misappropriating funds.
- Deliberately misrepresenting/concealing/ not disclosing one or more material facts relevant to any decision/transaction, financial or otherwise.
- 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.

c) **Red Flag Indicator or RFI** means a possible warning sign, that points to a potential fraud and may require further investigation or analysis of a fact, event, statement, or claim, either alone or with other indicators. List of red flag indicators are attached in Annexures below which is only indicative and not exhaustive in nature:

d) **Cyber or New Age Fraud** means any insurance fraud carried out using digital or new age technologies.

e) **"Distribution channel"** for purchasing insurance products, includes individual agents, corporate agents, insurance brokers, web aggregators, insurance marketing firms, Common Service Centres, etc. Authorized distribution channels to sell insurance products may be verified from the respective websites of insurance companies whose products are offered for sale

2. Fraud Classification –

To adequately protect itself from the financial and reputational risks posed by insurance frauds, IndusInd Nippon Life insurance (INLIC) has in place this framework to protect the insurer from the threats posed by the following broad categories of frauds.

2.1 Internal Fraud: Fraud involving internal staff, including employees and / or senior management.

2.2 Distribution Channel Fraud: Fraud involving distribution channels.

2.3 Policyholder Fraud and/or Claims Fraud: Fraud involving any person(s), in obtaining coverage or payment during the purchase, servicing, or claim of an insurance policy.

2.4 External Fraud: Fraud involving external parties' / service providers / vendors etc.

2.5 Affinity Fraud or Complex Fraud: Fraud involving collusion among one or more fraud perpetrators in the above categories

3. Fraud Risk Management:

IndusInd Nippon life Insurance 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 but not limited to below:

3.1. Prevention & Detection

Fraud prevention is the implementation of a strategy to proactively identify 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 fraud 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, red flag indicators, 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, creating test scenarios and providing output on various alerts.

- **Training & Awareness***:* To embed risk culture in organization, the Fraud risk team must create fraud risk awareness through training and communication to its employees, senior management including the board members, 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 and general public well about fraud awareness and solicit their participation in various preventive / detective measures

- ***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.

- **Vendor Engagement**: The organization's process is to perform all the required due diligence of Vendor onboarding by taking all the relevant approvals from the relevant stakeholders.

- **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).

- **Insurance Information Bureau (IIB)** – As a part of fraud prevention, IIB data is being used to find out suspicious policies of customers who have decline or rejected history with other insurers, this helps in early detection of potential frauds. As an organization, we also share data with IIB to enable industry to combat fraud and protect policyholders and all stakeholders.

- **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.

- **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:

Cyber Fraud means any insurance fraud carried out using digital or new age technologies. 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.

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 IRDAI, Cert-In, Life Council, IIB or Authority / Industry level forum 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. Annual report of Fraud risk assessment will be submitted to the Board of Directors through BRMC with all its findings and key highlights.

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 includes but not limited to CMU, Whistleblower, Pre-post issuance investigations, Escalated Customer complaints, CEO/CXO/HODs group, branch, legal, social media and self-Identified etc. Fraud Monitoring Unit (FMU) officers will be the designated officers for reporting incidents of fraud and report submission.

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. FMU will ensure that the investigations are conducted in an impartial manner. FMU 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. TAT of investigation must be maintained at extant as per IRDAI guidelines (wherever applicable) or Internal Processes on all fraud investigation cases.

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

Report Creation: - 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 can include sections like background, Scope, Investigation approach, findings and recommendations if any on case-to-case basis

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

Repository: - Investigation report shall be stored 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:

Corrective actions:

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

Legal Action/Recovery efforts Post investigation based on evidence if it has been proven that there is financial/reputational loss to INLIC, then corrective actions may be taken for recovery from fraudster and if required legal action would be initiated..

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 INLIC 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.

Revisiting & re-evaluate Underwriting decision to prevent company from fraudulent claims w.r.t Regulatory changes on IRDA regulation/Master Circular- Point no: 23- IRDAI (Protection of Policyholders, Interests, Operations and Allied matters of Insurers). Regulations,2024

3.5. 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.
- FMC submits quarterly report to the BRMC on its activities, findings, and recommendations including the financial impact of fraud on the insurer.
- Annual Comprehensive Fraud Risk Assessment before the Board of Directors through BRMC
- Report to the Audit Committee, in addition to the BRMC, in case of all internal frauds

External Reporting The Organization submits Annual report on fraud cases to IRDAI in forms FMR-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. RCA to be done on case to case basis.

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

Fraud Monitoring Committee (FMC): FMC shall be responsible for operationalizing the Fraud risk management Policy & framework and oversee activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remedying.

FMC composition to include following members

1. Chief Risk Officer,
2. Chief Operating Officer/ Head of Operations
3. Head-Legal
4. Chief Compliance Officer
5. Head Underwriting

Head of the department or any senior representative of related business group/department shall be the invitee to the Committee, with the permission of the members.

Quorum of the Committee - In order to constitute of valid quorum, presence of three Members is required.

Frequency: Atleast once a Quarter or as deemed necessary.

Functions of FMC - Recommend and regularly update, based on experiences, appropriate measures on fraud risk management to various functions. Oversee prompt responses to instances or suspicions of fraud. Maintain all relevant details pertaining to each instance of fraud. Facilitate collaboration with industry peers / bodies, law enforcement agencies and regulatory bodies to pursue cases of fraud and share information / intelligence on known fraud schemes and perpetrators. Conduct an Annual Comprehensive Fraud Risk Assessment to identify potential vulnerabilities across business lines and activities for fraud, using past experiences, emerging trends & Red Flag Indicators (RFIs), etc. Identify areas for improvement and adaptation of the Fraud Risk Management Framework.

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.

Fraud Monitoring Unit (FMU)– It discharges functions of fraud monitoring committee. 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. FMU also need to ensure the effective communication and awareness about fraud risk within the organisation. FMU must have disciplinary action matrix in place to take actions on agents/intermediaries for malpractices if proven.

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.

Zonal Ethics & Disciplinary Committee –ZEDC is conducted monthly and reviews the investigated cases and recommends the actions to CEDC

Central Ethics & Disciplinary Committee – CEDC reviews the recommendations of ZEDC and takes the final decision. Frequency – Once a month/as required.

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.

Appropriate and relevant due diligence must be undertaken by all employees from respective functions as per approved SOPs, in order to comply with regulatory guidelines.

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, senior management including the board members, intermediaries, vendors, customers and general public. Attention to be paid to the employees working in high-risk profiles/process to mitigate fraud risk. The Organization will also educate its customers and general public 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 Crisis Management Plan
- Information and Cyber Security Policy
- HR policies

7. Amendments and Review

This document will be reviewed at least annually and the changes to the Policy/Framework, if any, will be approved by the Board.

8. Annexures & Templates

- -Malpractice Action Matrix
- FMR
- Indicative Red flag indicators list

8.1. Malpractice Action Matrix

Action Matrix- Responsibility Nowover concept.

Risk case	Sub Category	First Level of Sourcing				Second Level of Sourcing				Third Level of Sourcing				Fourth Level of Sourcing			
		further investigation	1st instance	2nd instance	3rd instance	further investigation	1st instance	2nd instance	3rd instance	Condition (time span 6 months)	1st instance (25Mr)	2nd instance (45Mr)	3rd instance (65Mr)	Condition (time span 1 year)	1st instance (65Mr)	2nd instance (85Mr)	3rd instance (105Mr)
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 SIVs/ 3 instances	Warning	Termination		2 or more TIVs/ 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 SIVs/ 3 instances	Caution	Warning	Termination	2 or more TIVs/ 4 instances	Caution	Warning	Termination
	Insuring a dead person	Prior to March 2010	Termination			Prior March 2010	Warning	Termination									
		Post March 2010	Termination			Post March 2010	Termination			2 or more SIVs/ 3 instances	Warning	Termination	-	2 or more TIVs/ 4 instances	Warning	-	-
	Any terminal/ pre-existing disease which is apparent		Termination				Warning	Warning + Demotion	Termination	2 or more SIVs/ 3 instances	Warning	Termination	-	2 or more TIVs/ 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 SIVs/ 3 instances	Warning	Termination	-	2 or more TIVs/ 4 instances	Warning	-	-
	Early death claims	3 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 SIVs/ 3 instances	Warning			2 or more TIVs/ 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 TIVs/ 4 instances	Caution	-	-
Malpractice complaints	Signature, Medical, Proposal form, Documents submitted by client	No financial impact	Warning	Termination		No financial impact	Caution	Warning	Termination	2 or more SIVs/ 3 instances	Caution	Warning	Termination	2 or more TIVs/ 4 instances	Caution	-	-
		Financial impact	Termination			Financial impact	Warning	Warning + Demotion	Termination	2 or more SIVs/ 3 instances	Warning	Termination	-	2 or more TIVs/ 4 instances	Warning	-	-
	Illegal method of business	No financial impact	Caution	Warning	Termination	No financial impact	Caution	Warning	Termination	2 or more SIVs/ 3 instances	Warning	Termination	-	2 or more TIVs/ 4 instances	Warning	-	-
		Financial impact	Termination			Financial impact	Warning	Warning + Demotion	Termination	2 or more SIVs/ 3 instances	Warning	Termination	-	2 or more TIVs/ 4 instances	Warning	-	-
Submission of fake documents	Documents submitted are forged/fake		Termination		-	Financial impact	Warning	Warning + Demotion	Termination	2 or more SIVs/ 3 instances	Warning	Termination	-	2 or more TIVs/ 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 SIVs/ 3 instances	Warning	Termination	-	2 or more TIVs/ 4 instances	Caution	-	-
		Financial gain	Termination		-	Financial gain	Termination		-	2 or more SIVs/ 3 instances	Termination	-	-	2 or more TIVs/ 4 instances	Warning	-	-
Inhaus 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 SIVs/ 3 instances	Caution	Warning	Termination	2 or more TIVs/ 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 SIVs/ 3 instances	Caution	Warning	Termination	2 or more TIVs/ 4 instances	Caution	Warning	Termination
ease note the following:-																	
for anyone with vintage > 3 years, the action will be one level below for all cases - Except for death/ non insurance cases post March 2010																	
n Death/ non insurance cases post March 2010 and the vintage > 3 years (Both inclusive) - the Overall business participancy and no. of claims will decide the action as per the matrix on one level below																	

8.2. FMR Template

FMR – 1

Fraud Monitoring Report

Name of the Insurer:

Part I

Frauds Outstanding- Business segment wise:

Sl. No.	Category 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 (` lakh)	No.	Amount involved (` lakh)	No.	Amount involved (` lakh)	No.	Amount involved (` lakh)
	Internal Fraud								
	Distribution Channel Fraud								
	Policyholder and/or Claims Fraud								
	External Fraud								
	Affinity Fraud or Complex Fraud								
	Total								

In addition to the above, irrespective of the category of fraud, details of Cyber / New Age Fraud shall be reported separately in the following table.

Sl. No.	Brief description of Cyber Fraud (nature of data used to carry out the fraud, modus operandi, etc)	Financial Impact	Other relevant details

Part II – Age-wise analysis of unresolved cases

Sl. No.	Unresolved Cases at the end of the year (age-wise)	No.	Amount involved (` lakh)
1	30-60 days		
2	60 – 180 days		
3	180 – 360 days		
4	More than 360 days		
	Total		

Part III

Cases Reported to Law Enforcement Agencies

Sl. No.	Description	Unresolved Cases at the beginning of the year		New cases reported during the year		Cases closed during the year		Unresolved cases at the end of the year	
		No.	` lakh	No.	` lakh	No.	` lakh	No.	` lakh
	Cases reported to Police								
	Cases reported to CBI								
	Cases reported to Other agencies (specify)								
	Total								

8.3. Indicative RFI list as referred in IAIS Application Paper

a. The internal control structure is weak.
b. Training programmes are weak.
c. The organisational structure is too complex.
d. Internal audits do not exist or are weak.
e. The policyholder has several policies with the same insured object and coverage.
f. The claimant request payment to be made to a third party.
g. The policyholder changes insurer frequently.
h. The policyholder has been denied insurance before and has not mentioned this when applying for insurance.
i. There is different handwriting on various receipts.
j. There are inconsistencies between the application form and the claim form.

The list is only indicative in nature and not an exhaustive list and the applicability of each indicator to be evaluated.

End