Go Digit Life Insurance Limited

Anti-fraud Policy

Table of Contents

Sr. No.	Particulars	Page No.
A	Preamble	3
B	Applicability	3
C	Definition, scope and classification of frauds	3
D	Constitution of Fraud Control and Monitoring Unit	5
E	Principles to be followed in Fraud Monitoring Framework	6
F	Fraud Management Committee (FMC)	7
G	Procedures for fraud monitoring	8
H	Procedure for monitoring other frauds	9
I	Co-ordination with law enforcement agencies	10
J	Framework for exchange of information	10
K	Due Diligence	10
L	Regular communication channels	10
M	Consequences of failure to comply with the Policy	11
N	Handling of Frauds	11
O	Confidentiality and Non – Retaliation	11
P	Preventive Mechanism	11
Q	Anti-Fraud Officer	11
R	Potential RFIs	12
S	Regulatory Reporting	12
T	Training, Education and Awareness	12
U	Review of the Policy	12
	Annexure A	13
	Annexure B	15
	Annexure C	16

Go Digit Life Insurance Limited

Anti-fraud Policy

A. Preamble

This Anti-fraud policy ("Policy") is being framed for fraud prevention and detection and is established to facilitate the development of controls which will aid in the detection and prevention of fraud against Go Digit Life Insurance Limited ("Digit/Company"). Digit has "Zero tolerance" approach towards any fraudulent act committed against its policy holders, shareholders, employees and associates. Through this Policy, Digit intends to promote consistent organizational behaviour by providing guidelines and setting a responsibility matrix for the development of controls and conduct of investigations.

To provide regulatory supervision and guidance on the adequacy of measures taken by insurers to address and manage risks emanating from fraud, the IRDAI vide IRDAI (Insurance Fraud Monitoring Framework) Guidelines, 2025 [Ref No: IRDAI/IID/GDL/MISC/112/10/2025] effective April 1, 2026 ("Circular") laid down the Guidelines requiring insurance companies to target zero tolerance for fraud and put in place appropriate Fraud Risk Management Framework to deter, report and remedy Insurance Frauds.

Accordingly, this Policy lays down the framework adopted by the Company to implement mitigation measures and pro-active fraud detection framework. This Policy also aims to protect the brand, reputation and assets of the Company from loss or damage, resulting from suspected or confirmed incidents of fraud/misconduct. The policy seeks to establish and maintain a robust framework to provide reasonable assurance that dishonest or fraudulent acts are promptly detected and actioned upon. The objective is to promote an ethical and fraud-free environment at the Company.

B. Applicability

The Policy would apply to all employees of the Company, to persons appointed on adhoc/ temporary/ contract basis, trainees, apprentices, representatives of business associates, vendors, intermediaries, customers, as well as others doing business or having dealings with the Company. The contractual agreements with the employees/intermediaries shall include an appropriate provision for governing them by this Policy.

C. Definition, scope and classification of frauds

Fraud is a term which generally refers to any act committed intentionally to secure an unfair or unlawful gain. This wrongful gain through deceit can be made either singly or jointly with others.

Frauds can be committed by clients, intermediaries, impostors, petitioners, third party administrators, vendors and even by the internal staff of the companies. Apart from that professional syndicates operate all over the country.

The frauds that could be perpetrated against the Company inter alia includes embezzlement, bribery, vendor related third party frauds, money laundering, etc. The risk of employees tinkering with the confidential information and colluding with fraudsters is also prevalent.

Reasons for the frauds are mainly:

- Opportunity of getting very high rewards with minimal possibility of detection
- Penal provisions extremely soft having very low prosecution
- Victimless and easy to commit
- Insurance frauds are hardly considered as social stigma. In fact, most of these are taken as accepted practice by the society

Go Digit Life Insurance Limited

Anti-fraud Policy

- Insurance frauds are very low on priority for law enforcement agencies
- Opportunity for the business houses in distress to compensate for the losses
- Weak internal systems & processes
- Lack of effective vigilance and investigation mechanism

Fraud in insurance or **Insurance Fraud** shall mean an act or omission intended to gain dishonest or unlawful advantage for a party committing the fraud or for the other related parties.

For instance, Insurance Fraud may be perpetrated by means of:

a) misappropriating assets;

b) deliberately misrepresenting, concealing, suppressing or not disclosing one or more material facts relevant to a financial decision, transaction or perception of the status of Digit;

c) abusing responsibility, a position of trust or a fiduciary relationship.

Red Flag Indicator/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.

Distribution Channel include insurance agents, intermediaries or insurance intermediaries, and any persons or entities authorized by IRDAI to involve in sales and service of insurance policies.

Cyber or New Age Fraud means any Insurance Fraud carried out using digital or new age technologies.

Law Enforcement Agencies (LEA) shall mean any governmental authority or agency legally empowered under applicable laws, including the Prevention of Money Laundering Act, 2002 (PMLA), to investigate, prevent, or prosecute offences. This includes, but is not limited to:

- Enforcement Directorate (ED) and officers appointed under Sections 48 and 49 of PMLA
- Police authorities at State and Central levels
- Customs and Central Excise Departments
- Income Tax Department
- Securities and Exchange Board of India (SEBI)
- Any other statutory or regulatory body notified under Section 54 of PMLA or other applicable laws.

Classification of Fraud:

Fraud may be broadly categorized as below:

- Policyholder Fraud including Claims Fraud: Fraud against the insurer in the purchase and/or execution of an insurance product, including fraud at the time of making a claim.
- Distribution Channel / Intermediary Fraud: Fraud perpetuated by an insurance/micro-insurance agent, Point of Sales Person (POSP), insurance intermediary including any of the employees of such intermediary against the insurer or policyholders;

- Premium siphoning: This is generally done at the point of sale by the direct sales force and by the channel partners. Misuse of credit card details by the call centre executives for this purpose is also common. Modus operandi is simple i.e. to collect the premium in cash from the unsuspecting customers and pocketing it and in return hand them over fake or manipulated policy documents. This is noticed mostly when such customers prefer claims or at the time of endorsement / renewal of policy.
- Commission siphoning: Releasing excess commission and then subsequently receiving kickback out of it. Creation of dummy deals in the names of fictitious persons / family members to book direct business into indirect; consolidate commission under particular agent and then illegally pocketing it. Deals of agents who are no longer willing to work with the company are kept active and misused for diverting commissions.
- Internal Fraud: Fraud/ misappropriation against the insurer and/or any of its policyholders by its Director, Manager and/or senior management and/or any other officer or staff member
- External Fraud or Fraud by Third Party: Fraud committed by third parties / service providers / vendors against the Insurer and/or the general public which primarily includes activities such as issue of fake/forged policies and cover notes in the name of the Insurer
- Aadhaar-related Fraud: Fraud committed related to Aadhaar information of customers, agents, intermediaries, employees, staff members, etc.
- Affinity Fraud or Complex Fraud: Fraud involving collusion among one or more fraud perpetrators in the above categories.

D. Constitution of Fraud Monitoring Unit

The Company shall constitute a Market Conduct team to act as a Fraud Monitoring Unit (FMU) for implementing the Fraud Risk Management Framework through the respective functions. FMU must operate independently under Head Legal & Compliance. The FMU shall be supported by the respective function in carrying out the activities required under the Policy including Underwriting, Claims, Operations, Finance, Grievance, Risk, Human Resource, Internal Audit. SPOCs from Other Functions shall be made/considered part of the FMU for performing the activity required under the Policy. The Company may lay down any additional fraud management processes and procedures as may be appropriate. It shall report the status of significant cases of fraud detected in the Company to the Fraud Management Committee and to the Board of Directors/ Board appointed Committee on a annual basis.

Functions of FMU with the support of the respective function shall include but not be limited to the following:

- Identify Potential areas of Fraud: actively try to identify potential areas of fraud. It shall undertake data analytics to find any fraud patterns and subject the same to field investigation. Further, it shall also analyse the data based on frauds detected during field investigations.
- collate all cases of frauds reported to it by the Whistleblower Complaints Committee (WBCC) or any other entities.
- investigate all such cases and render report to the WBCC duly highlighting the breaches of conduct, process and system etc. Report shall also highlight the financial implication, if any.
- implement the decisions by FMC
- track the closure of the decisions through Action Taken Report (ATR).

- get the cases having involvement of non-related entities reviewed and closed through President –Retail Business and submit details of such cases to the FMC.
- Due Diligence: The HR Department shall conduct due diligence of employees at the time of on-boarding. The due diligence of intermediaries, channel partners, vendors, Hospitals, Garages etc. shall be carried out by the respective departments.
- Reporting: FMU shall lay down the procedure for internal / external reporting from / and to various departments.
- Creating Awareness: FMU shall take steps to create awareness through periodic communication and training programs among the employees, intermediaries, policyholders to counter insurance frauds.
- take appropriate steps to share information pertaining to fraud cases amongst all insurers, regulators, government authorities and to co-ordination platforms as may be made available at any time by Life Insurance Council or IIB etc.
- In performing their duties under this Policy, the members of the FMU will have free and unrestricted access to all Company records and premises, whether owned or rented, and the authority to examine, copy and/or remove all or any portion of the contents of files, desks, cabinets and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation, subject to approval Anti-Fraud Officer.
- The Department Heads shall be responsible to take actions as per the decision of the FMC. Further, the Departmental Heads shall be responsible to act on the recommendations of FMU which it may render from time to time to improve any System and Process gaps.

E. Principles to be followed in Fraud Monitoring Framework

- Principle of proportionality: In taking anti fraud measures, the Company must recognise the principle of proportionality i.e. the measures adopted to mitigate frauds must be in proportion to the risks involved.
- Zero tolerance: Any activity with the intention of perpetuating fraud against the Company shall not be tolerated. Any individual involved in a fraudulent activity will be subject to sanctions up to and including dismissal from services of the Company. The Company may further take criminal or civil proceedings under applicable laws. In case of agent/intermediary/Vendor/TPA who fail to adhere to this Policy, the Company may terminate its relationship with them or may further take criminal or civil proceedings under applicable laws.
- Full investigation: Suspected fraudulent activity must be investigated immediately by FMU. Where this cannot be done internally, FMU may use external consultants or seek assistance of government bodies. If the investigation establishes a strong suspicion of violation of the law, the Company reserves the right to take any action including but not limited to civil and criminal prosecution.
- Compliance with law and internal policies: The Company shall ensure that while implementing the anti-fraud measures, the applicable laws and internal policies of the Company must be strictly complied with. This also applies where the help of external consultants is taken to investigate a case of fraud.
- Documentation: Anti-fraud management activities and measures must be clearly documented and records maintained for 10 years. Where a case of fraud is the subject of investigation, care must be taken to ensure that, as far as possible, all evidence is available in a form admissible in court.

- Regular review and refinement: The components of anti-fraud management and associated measures, especially the effectiveness of internal controls, must be reviewed on a yearly basis.

F. Fraud Management Committee (FMC)

FMC shall be constituted to review the findings of the investigations done and to take appropriate actions thereupon. The FMC shall be responsible for operationalizing the Fraud risk management framework within the insurer and oversee activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remedying.

Composition of FMC:

The FMC shall comprise of

1. Head Legal & Compliance (Head of FMC)
2. Head of Claims
3. Head of Underwriting
4. Head of Operations
5. Chief Finance Officer
6. Chief Risk Officer
7. Grievance Redressal Officer

The FMC may also form sub-committees, as required, for effective functioning.

FMC may invite other Officials as may be required.

The Composition of FMC may be changed with the approval of the MD & CEO.

G. Procedures for fraud monitoring

This may includes prevention, detection and response (investigations and reporting) while focusing more on fraud prevention and a proactive approach towards mitigating fraud risk. Department / Function wise illustrative list of frauds & control procedures may be prepared as per requirement. FMU may put in Place the SOP.

I. Fraud prevention

(a) Following activities may be undertaken towards fraud prevention:

- Fraud Risk Assessment
- Training on code of conduct, anti-fraud policy, Anti Money Laundering, Anti Bribery/Corruption, etc
- Board Approved Whistle Blower Policy as adopted by the Company
- Employee and third party due-diligence
- Data analytics and documents review

(b) The Fraud Monitoring function shall be responsible for deciding on the content and periodicity of training/information to be imparted.

(c) Employees shall have the responsibility to recognize potential fraud and should be familiar with the types of improprieties that might occur within his/her area of responsibility and be alert for any indication of irregularities.

(d) Each department shall be responsible for their business processes in order to identify and prevent potential fraud. Every Head of the Department shall be responsible to cascade relevant information to the employees working under his/her department.

II. Identification

a) In addition to Head of each department and employees' responsibility to report fraud, the FMU with the support of the respective function shall implement processes to identify frauds and discharge its functions with effective implementation of measures suggested by FMC.

b) The nature and extent of fraud risk assessment shall commensurate with the size of the Company's business/operations and complexity and shall be performed at all appropriate levels within the organization (i.e. entity level; significant account balance or business cycle/process level; and significant locations or business units).

c) Risk assessment or audit shall be performed, documented and updated periodically to identify potential fraud schemes, scenarios and events that need to be mitigated.

d) Updates shall inter alia include considerations of changes in operations, new information systems, changes in job roles and responsibilities, internal audit findings, new or evolving industry trends.

e) The Company shall adopt appropriate procedures to identify "missed" insurance fraud detection opportunities.

Annexure A provides an illustrative list of actions constituting fraud.

III. Fraud Investigation, Fact Finding & Corrective Action

a) The Company shall through the relevant function(s) initiate suitable actions in response to an alleged or suspected incident of fraud:

   1) Conduct thorough investigation of the incident.

   2) Take appropriate and consistent action(s) against violators including legal recourse where deemed necessary.

   3) Identify areas of improvements in relevant controls.

b) Investigation shall be carried out without having any prejudice towards the incident which is being investigated and/or the accused.

c) Focus of investigation should also be towards weeding off any malicious or mistaken accusations.

d) FMU and the SPOCs engaged from other functions will have access to necessary records and premises, whether owned or rented, and the authority to examine, copy and/or remove all or any portion of the contents of files, desks, cabinets and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation.

e) The investigation shall be conducted in a fair manner and shall be focused on neutralisation process to minimize losses and prevent any suspected party from covering-up the fraud.

f) The person alleged will be informed of the allegations as soon as reasonably practicable. This may not be until the initial stages of the investigation have taken place.

H. Procedure for monitoring other frauds

Any cases of embezzlement of cash / assets found shall be dealt with as per the provisions contained in the Code of Conduct through FMU

Trainings shall be imparted to all new joiners during induction program on arms-length principles as contained in the Code of Conduct

The Company shall conduct regular awareness campaign on Frauds related to embezzlement of cash / assets to all employees including off roll employees, if any.

Cyber or New Age Fraud: The FMU in conjunction with the IT department shall

- Establish and implement robust cybersecurity framework to protect against evolving cyber frauds or threats.
- Continuously monitor and strengthen systems and processes for fraud risk management, such as incident databases, customer verification, and access control.
- Putting in place a qualified risk and technology expert to manage cyber fraud risks across all lines of business.

I. Co-ordination with law enforcement agencies

The Company shall extend necessary support to Government, law enforcement agencies and international bodies in their efforts to combat the use of financial service Industry for perpetrating fraudulent activities. Any public communications and comments by or on behalf of the management to the press, law enforcement agencies or other external parties in relation to incidents of fraud shall only be made by Digit's authorized personnel in co-ordination with the legal team.

J. Framework for exchange of information

The Company shall suo motu provide information to other insurance companies, either directly or through Insurance Council, in case there is a possibility of impact on such other insurance companies as well. Any call for information made by IRDAI or the Insurance Council shall be promptly responded by the Company.

K. Due Diligence

The Company has put in place due diligence requirements while onboarding employees and engaging partners, third party vendors. The Company's Outsourcing Policy provides in detail the due diligence measures to be carried out while entering into arrangements with third party vendors for material activities falling under Outsourcing. In particular, the Company shall have requisite standard operating procedures in place with respect to the due diligence and empanelment of insurance agents and insurance intermediaries and should strictly abide by the same.

Prior to empanelment of an insurance agent or entering into an agreement with any insurance intermediary, the Company shall carry out requisite due diligence considering factors such as security, business continuity, etc. wherever applicable. The FMC/FMU may suggest documents/information (as indicated in Annexure B) that may be collected from all/some or identified intermediaries (proposed to be empanelled), based on the judgement of the 'Designated Person' (as authorized pursuant to IRDAI requirements).

In case of default, appropriate actions shall be undertaken against the insurance agent / insurance intermediaries as per applicable IRDAI Regulations and terms of the agreement.

L. Regular communication channels

The Company shall periodically as well as on adhoc basis sensitize employees through communication/training with a view to reinforce the Company's values, code of conduct and expectations. Necessary information shall also be given to the concerned departments which have an impact due to the fraud to put in place appropriate controls for avoiding repetition of such instances in future. The Fraud Monitoring Function shall also relay information to the Board or any of the Board delegated committees as deemed fit.

Any employee, customer, shareholder or other interested parties aware of or with reason to believe a violation of practices or procedures exists including involving the financial reporting of the Company, internal accounting reporting or auditing matters or operational matters should notify the Company by writing in the manner provided by the Company.

M. Consequences of failure to comply with the Policy

The Company expects all its employees to act in full compliance with this Policy in conjunction with the Code of Conduct, Whistleblower Policy and such other policies in a manner consistent with the highest ethical standards. This Policy and its relevant provisions shall be adequately publicised and made known to all concerned including employees, agents, intermediaries and other channel partners.

Any employee found to have been involved in a fraudulent activity or other misconduct or to have failed to report a known or suspected instance of Fraud will be subject to disciplinary action up to and including termination. Furthermore, such conduct of the employees or other parties if found to be in violation of the law then it may result in civil or criminal action.

All vendors, intermediaries and others dealing with the Company shall adhere to this Policy. Failure to adhere to this Policy may result in appropriate actions as prescribed under this Policy including but not limited to termination of relationship.

N. Handling of Frauds

FMU and Respective function shall be responsible for handling all Frauds that are reported to the Company. It shall take prompt and appropriate action with respect to such frauds to remediate the circumstances giving rise to occurrence of such frauds. While handling frauds, FMU shall be guided by directions issued by FMC, if any.

O. Confidentiality and Non – Retaliation

Under the Policy, every reasonable effort shall be made to ensure the confidentiality of the person who has reported the Fraud. The identity of those providing information shall be kept confidential in order to carry out an appropriate, fair and thorough investigation. If a fraud is reported anonymously, the person must provide credible and sufficient information to enable the FMU to investigate. The Company shall ensure that no retaliatory action is taken against any individual for reporting, in good faith, known or suspected Fraud.

P. Preventive Mechanism

In addition to measures mentioned in the Policy, the Company shall have in place appropriate clauses in agreements, appointment letters, proposal forms, policy documents to highlight the importance of correct disclosure and consequences of wrongful disclosure/concealment. The Company shall periodically run appropriate awareness campaign against frauds for all its' employees. A brief training on prevention of frauds shall be imparted to all new entrants during the induction training. All employees shall be required to confirm their adherence to this Policy and declare any Conflict of Interest, once in a year.

Q. Anti-Fraud Officer

The Head of Legal & Compliance shall be nominated as the Anti-Fraud Officer of the Company. The MD and CEO is authorised to nominate any other official as Anti-Fraud Officer of the Company. Any deviation of the Policy shall be reported Life.Compliance@godigit.com.

R. Potential RFIs

The Company shall treat such facts, events or situations as RFIs as mentioned under Annexure C. These RFIs shall be reviewed regularly for their continued relevance and effectiveness in detecting fraud by the Company. The existence of these warning signs or indicators does not mean that internal fraud has occurred or shall occur. Nevertheless, the Company shall look out for these warning signs or indicators, particularly when more than one of such signs occurs.

S. Regulatory Reporting

A. IRDAI

The Company shall submit information to the Authority with respect to fraudulent cases in the formats and timelines as may be prescribed by the Authority from time to time. Based on the information provided the Company shall submit report to IRDAI in forms FMR 1 providing details of outstanding fraud cases and closed fraud cases every year within 30 days of the close of the financial year in the prescribed format as specified by IRDAI from time to time. In the event of fraud committed by distribution channels registered by IRDAI, the Company shall promptly escalate and report the matter to IRDAI without delay.

B. IIB

To curb and prevent frauds in Industry Level, the Company shall participate in the Fraud Monitoring Technology framework and make available to IIB (Insurance Information Bureau) all such information of frauds detected to combat fraud at an industry level. We shall share to IIB all the details of distribution channels, hospitals, third party vendors and fraud perpetrators blacklisted, and share records of the fraudulent activities noted. In addition to these reporting obligations, the Company shall, always, fully cooperate with Law Enforcement Agencies (LEAs) by promptly facilitating any requirements raised and providing complete details of all reported and recorded fraud incidents upon request.

T. Training, Education and Awareness

The Company shall conduct:

(a) Regular Fraud Awareness programs to educate policyholders and the general public about the risk on fraud and how to prevent and protect against it through internally coordinating with marketing team in the form of campaigns.

(b) Periodic Training Programs to the employees and the senior management including board members by coordinating with internal Human Resources and Learning and Development Department, as may be appropriate.

(c) Training Programs through internal distribution departments.

U. Review of the Policy

This Policy shall be reviewed by the Risk Management Committee annually or at any other frequency as may be deemed necessary or as and when the underlying laws governing the Policy undergo any change. This Policy may be modified by the Managing Director and CEO and Head – Legal & Compliance of the Company jointly prior to any such review by the Risk Management Committee and such modifications shall be reported to the Board at its next meeting for approval / ratification. Any requirement under the law, to the extent applicable to the Company, that needs to be covered under the policy or any changes in the applicable laws, to the extent applicable, shall be deemed to be incorporated into this policy automatically.

Annexure A

Illustrative list of actions constituting fraud

Some of the examples of fraudulent acts/omissions include, but are not limited to the following:

1. Internal Fraud:
   a) misappropriating funds
   b) fraudulent financial reporting
   c) stealing cheques
   d) overriding decline decisions so as 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 kickbacks/favours
   h) forging signatures
   i) removing money from customer accounts
   j) falsifying documents
   k) selling Company's assets at below their true value in return for payment.

2. Policyholder Fraud and Claims Fraud:
   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

3. Distribution Channel / Intermediary fraud:

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

b) Inflates the premium, passing on the correct amount to the Company 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 Company, collecting commission and annulling the insurance by ceasing further premium payments.

4. Aadhaar-related fraud:

a) Misuse of Aadhaar related to information / documents in custody of the Company by and off the customer, intermediary, Vendor and employees etc.

b) Fabrication of Aadhar documents and details submitted

c) Impersonation of Aadhar information as well as details

d) Usage of stolen or fabricated Aadhaar numbers for fraudulent policy issuance.

Cyber / New Age frauds:

(a) Loss of Confidential Data: Personally identifiable information collected and stored by the Company, including personal information of policyholders and, in some cases, of third parties.

(b) Sensitive Information being compromised: Insurers may collect sensitive business information that could be valuable to corporate / foreign spies. In the case of certain lines such as cyber insurance products, the Company may possess information about a policyholder's network security controls and other cyber resilience information that could be valuable and could harm intellectual property rights of either party.

(c) Disruption of Operations: Cyber-attacks can result in disruption to normal business operation including emails, telephone directories, and voice mails amongst business records such as contract templates.

(d) Loss of Trust: The foundation of insurance business is policyholder trust that the information collected by insurers will be protected, and trust that claims will be paid out in a timely way when appropriate. If an insurer were to suffer a cyber security incident that rendered it unable to make timely claims payments that trust may also be shaken. The reputational risk could extend to the sector as a whole.

Go Digit Life Insurance Limited

Anti-fraud Policy

Annexure B

The documents/information that may be collected from all/some or identified intermediaries

Insurance Agent:

Before recruiting an agent, below requisite documents as applicable from time to time shall be obtained

IRDAI Form - signed by proposed agent based on PAN:

Form IA (Fresh case)

Form IB (Composite case)

Form IA & IC (Transfer case)

Form IB & Form IC (Transfer + Composite case)

Other documents:

PAN card copy/Aadhaar card copy / Address proof

Education proof - 10th mark sheet(minimum)

Cancelled cheque

Corporate Agent:

Before entering an arrangement with a Corporate Agent, following documents shall be obtained:

1. A written agreement shall be entered into between the Company and the Corporate Agent as required under and in terms of the provisions IRDAI (Registration of Corporate Agents) Regulations, 2015.
2. Copy of IRDAI registration certificate of the Corporate Agent, Corporate Agent's address proof and PAN card copy, details of the Principal Officer.

Annexure C

Illustrative list of RFIs for the Company

Business practices and condition

- Insufficient information is available about prior audits.
- The internal control structure is weak.
- Management operations and financial decisions are dominated by a single person or by several people who generally act together.
- Tasks and/or transactions are very complicated, requiring special skills.
- There are indications of financial trouble, for example, inadequate capital or increase in unpaid debts.
- Training programmes are weak.

- The organisational structure is too complex.
- Internal audits do not exist or are weak.
- The Board has a very high proportion of executive directors.
- Members of the Board, Senior Management or other staff have external business interests and/or cosy relationships with contractors.
- Complaints or signals are received from external parties (like suppliers or customers) and/or there are missing statements and unrecognised transactions.
- Security systems for data and assets are weak.
- Sudden changes are made to the Company's strategy.
- Accounting is poor.
- Transactions, processes or expenses are poorly documented.
- Transactions are unusual as to time (for example, day of the week, season), frequency (too many, too few), place (too near, too far out), amount (too high, too low, too consistent, too different) and parties (related parties, strange relationships).
- Activities are not consistent with the Company's stated policies.