Anti-Fraud Policy

Aviva Life Insurance Company India Limited (Aviva India)

Policy Owner: Chief Legal & Compliance Officer, Aviva India
Board approved policy

Ver. 5.0_March 2026

Table of Contents

1. Introduction

Aviva India Insurance Company India Limited ("Aviva India") maintains a zero-tolerance approach to fraud, consistent with the *IRDAI (Insurance Fraud Monitoring Framework) Guidelines, 2025 (the "Guidelines")*, applicable to all insurers and distribution channels.

Aviva India is committed to:

- Upholding the highest standards of integrity and ethical conduct.

\

Safeguarding policyholders' interests.

- Protecting financial stability.
- Ensuring full compliance with legal and regulatory obligations.
- The continual improvement and enhancement of its Fraud Risk Management Framework ("FRMF").

This policy establishes a comprehensive, organisation-wide fraud risk management framework to deter, prevent, detect, report and remedy all forms of insurance fraud, in line with IRDAI's requirements.

2. Objectives

The objectives of this policy are to:

1. Maintain a Board-approved FRMF as mandated by IRDAI, and in line with all relevant applicable laws and regulations as amended from time to time.
2. Set out clear lines of accountability for managing fraud risk across all three lines of defence.
3. Ensure timely detection, remediation and reporting of fraud incidents to internal committees, the Board, IRDAI and relevant law-enforcement agencies.
4. Foster a culture of fraud awareness, supported by training, risk-based controls and proactive monitoring measures.
5. To build resilience against fraud, foster a culture of integrity, protect policyholders' interests, safeguard financial stability and maintain public trust.

3. Scope

This policy applies to:

- All employees, directors and contractual staff of Aviva India.
- Distribution channels (agents, intermediaries, corporate agents and brokers etc.).
- Vendors, service providers, consultants and third parties engaged by Aviva India.
- Policyholders, customers, beneficiaries and any person interacting with Aviva India.

It covers all actual, suspected or attempted fraud involving Aviva India or its stakeholders.

A suite of supporting documents underpins this policy, with key documents listed in Annexure 1.

4. Definitions

4.1 Cyber or New-Age Fraud

Fraud perpetrated using digital or emerging technologies, including phishing, identity theft, synthetic identity creation or system manipulation.

4.2 Distribution Channels

Agents, intermediaries or any person/entity authorised by Aviva India to market, solicit or service its insurance products, as defined in IRDAI regulations.

4.3 Fraud

Any act or omission intended to gain an undue advantage through dishonest or unlawful means, either for the person committing the act or for a related party including (but not limited to) misappropriation of funds, misrepresentation, concealment of material facts, or abuse of position of responsibility, trust, or fiduciary duty to obtain an improper benefit.

4.4 Fraud Monitoring Committee ("FMC")

Means the committee constituted at Aviva India, comprising the Chief Legal and Compliance Officer (Chairperson), the Chief Risk Officer, the Head of the People Function, and the Chief Technology Officer. The FMC operates in accordance with its approved Charter, which sets out its constitution, functions, and roles and responsibilities.

4.5 Fraud Monitoring Unit ("FMU")

Means the dedicated and independent unit established in accordance with the IRDAI Guidelines, responsible for supporting the FMC in deterring, preventing, detecting, reporting, and remedying fraud, and ensuring effective implementation of fraud-risk controls across Aviva India. The Group Investigations ("GI") function at Aviva India is designated as the FMU.

4.6 Key Managerial Personnel – "KMP"

KMP are members of Aviva's India core senior management team, including C-suite officers, key functional heads and other senior officers designated as critical to governance and control.

4.7 Red Flag Indicator – "RFI"

Any event, behaviour or information that may indicate potential fraud and warrants further assessment or investigation.

Examples of actions constituting fraud and RFIs are set out at Annexure 3.

5. Classification of Frauds

Fraud incidents must be categorised as follows:

1. **Internal Fraud** – fraud committed by Aviva India employees or senior management.
2. **Distribution Channel Fraud** – fraud involving agents, intermediaries or any person/entity authorised by Aviva India to market, solicit or service its insurance products.
3. **Policyholder / Claims Fraud** – fraud committed by policyholders or claimants during policy purchase, servicing, or claims to obtain an undue benefit.
4. **External Fraud** – fraud by third parties, vendors, service providers, hospitals, or other external persons/entities.
5. **Affinity / Complex Fraud** – collusion between multiple parties across any of the above categories; often sophisticated and/or coordinated.

6. Cyber or New Age Fraud

To seek to prevent Cyber and New-Age Fraud, Aviva India shall, *inter alia*:

- Establish and maintain a robust and comprehensive cybersecurity framework that protects the organisation against evolving cyber-enabled frauds and emerging digital threats.
- Continuously monitor, review, and enhance fraud-risk management systems and controls, including incident-tracking databases, customer identity-verification mechanisms, authentication protocols, and access-control safeguards.
- Deploy and utilise a dedicated team with appropriate risk, technology, and cybersecurity expertise to oversee, manage, and mitigate relevant cyber-fraud risks.
- Implement and enforce policies, procedures, and technological safeguards aligned with applicable IRDAI regulations and recognised industry standards for cybersecurity and fraud prevention.
- Ensure timely reporting and escalation of identified cyber-fraud risks, incidents, or vulnerabilities to the designated governance forums in accordance with regulatory and internal requirements.

7. Fraud Risk Management Framework

Aviva India maintains a comprehensive Fraud Risk Management Framework approved by its Board, in line with IRDAI's 2025 requirements for a "*full-spectrum deter-prevent-detect-report-remedy approach*". A high-level pictorial overview of the FRMF is set out in Annexure 2.

6.1 Governance Structure

6.1.1 Board of Directors

Primary accountability for fraud-risk governance, with its responsibilities including:

- Approves the Anti-Fraud Policy (this document).

- Oversees the overall FRMF, ensuring a zero-tolerance culture toward fraud is embedded across the organisation.
- Ensures appropriate governance structures are established, including the FMC and the independent FMU.
- Receives periodic reporting from the FMC, via the Risk Management Committee ("RMC") and Audit Committee to monitor fraud trends, systemic issues, and control enhancements.

6.1.2 Risk Management Committee (RMC)

Acts as the governance bridge between the FMC/FMU and the Board, with its responsibilities including:

- Responsible for the effective implementation and oversight of the FRMF.
- Receives reports from the FMC on fraud risks, investigations, emerging trends, annual Fraud Risk Assessment and control weaknesses.
- Oversees fraud risk as part of the broader enterprise risk management (ERM) framework, ensuring fraud risk is treated as a critical risk category.
- Reviews the effectiveness of fraud-risk controls, including oversight of cyber/new-age fraud exposure and resilience.

The RMC is governed by, and discharges its responsibilities in line with, the RMC Charter.

6.1.3 Audit Committee

Oversees Internal Audit assurance on fraud controls; reviews significant fraud matters; monitors fraud-related financial reporting risks; interacts with the RMC as necessary.

Receives quarterly reports on internal fraud through FMC.

6.1.2 Fraud Monitoring Committee ("FMC")

- Constituted as per IRDAI Guidelines and governed by the FMC Charter.
- Chaired by the Aviva India Chief Legal & Compliance Officer.
- Includes the following KMP members: Chief Risk Officer, Head, People Function, and Chief Technology Officer.
- Supported by the Fraud Monitoring Unit ("FMU") in fulfilling its responsibilities and ensuring the effective implementation and ongoing delivery of activities.
- Reports quarterly to the RMC and Audit Committee.

6.1.2 Fraud Monitoring Unit ("FMU")

- The Aviva India GI function is formally designated as the FMU.
- Supports the FMC in discharging its oversight responsibilities and ensuring the effective implementation of the FRMF and any measures recommended by the FMC.

- Implements and executes the procedures for conducting fraud-sensitive audits in identified high-risk areas, as outlined in the Annual Compliance Plan, and does so with support from the relevant functions and subject-matter experts as required. The outcomes of these audits are monitored to ensure timely corrective and preventive actions.
- Conducts a comprehensive annual Fraud Risk Assessment ("FRA") to identify potential fraud vulnerabilities across business lines and activities, drawing on past incidents, emerging fraud trends, RFIs, and other relevant intelligence.
- Engages and coordinates with law-enforcement agencies, supporting regulatory reporting, evidence sharing, and the progression of formal investigations where required.
- Investigations are conducted in accordance with GI's Standard Operating Procedure (SOP), which sets out the required internal processes, including inter alia defined case turnaround timelines.

6.1.3 Three Lines of Defence

- **1st Line:** The first line holds primary responsibility for executing and embedding effective fraud-risk management. This includes applying core risk-management principles—identifying, assessing, managing, monitoring, and reporting fraud risks as part of day-to-day business operations.
- **2nd Line:** The Compliance and Risk functions operate as the second line of defence, providing oversight, review, and challenge. They assess the completeness, quality, and robustness of the first line's fraud-risk identification, measurement, management, monitoring, and reporting activities, ensuring controls and processes are fit for purpose.
- **3rd Line:** Internal Audit acts as the third line of defence, delivering an independent and objective assessment of the design and operational effectiveness of the FRMF. Internal Audit also reports its findings, concerns, and recommendations to the Aviva India Audit and Risk Committees as appropriate.

Reviews carried out by the second and third lines will seek to identify missed and emerging fraud-detection opportunities, and opportunities for improvement, seeking to ensure the progressive strengthening of fraud-risk management capabilities.

Aviva India has incorporated appropriate control measures with respect to each category of fraud. An indicative list of such controls embedded in processes are set out in Annexure 3.

6.2 Fraud risk - system of controls and processes

Within the FRMF, Aviva India maintains a system of controls and processes that serves as a core governance mechanism to deter, prevent, detect, report, and remedy fraud risks across all business operations.

The various components of the system are regularly updated to reflect emerging fraud patterns, operational changes, and insights from investigations and other activities, in keeping with the requirement for a living FRMF reviewed at least annually.

This system constitutes an extensive and integrated fraud risk management framework, comprising the following key components (not exhaustive):

- **Aviva's Integrated Common Assurance Reporting Tool ("iCare")** – Aviva India uses an internal governance and reporting platform designed to provide a unified, structured mechanism for capturing, assessing, and reporting assurance-related activities across the organisation. The tool enables consistent oversight of risk, control effectiveness, compliance, and assurance findings by consolidating inputs from multiple assurance functions. Its use in respect of fraud risk includes, but is not limited to, capturing:
    - Identified fraud risks - All significant known or potential fraud risks identified across the functions and distribution channels, consistent with the IRDAI-mandated fraud classifications.
    - Existing controls and mitigating measures - A record of the key preventive and detective fraud controls in place, including the FRA, technology-enabled safeguards and cyber-fraud defences required by IRDAI to address evolving digital fraud risks.
    - Accountability and ownership - Assignment of control ownership to relevant functions/roles
- **RFIs** - Documented early-warning indicators signalling potential fraud, as defined by the Guidelines, requiring investigation or heightened monitoring. The FMU owns the RFI process note and is responsible for coordinating the identification, assessment, and management of RFIs, with support from relevant functions and subject-matter experts as required.
- **FRA** – This includes the classification of each fraud risk in accordance with IRDAI definitions and taxonomy, along with assessments of likelihood, impact, and inherent and residual risk levels. The FMU has responsibility for the FRA together with the corresponding process note.
- **Reporting and escalation of fraud concerns** – Documented mechanisms are in place for promptly escalating fraud incidents, concerns and risks, internally and externally. These avenues for reporting are detailed in Aviva India's Speak Up Charter (Whistle-blower Policy) – Speak Up being Aviva India's whistleblowing service.
- **A central fraud incident database** - Maintained and updated by the FMU, ensuring all fraud-related information is accurately recorded, tracked and reported in line with the Guidelines. The incident database also details the corrective and preventive actions initiated in all such instances.

8. Distribution Channel Fraud Framework

Aviva India requires all distribution partners to operate in accordance with a robust and proportionate fraud-risk management framework, ensuring full alignment with regulatory expectations and the Aviva India's zero-tolerance approach to fraud.

All distribution partners are required to comply with the following fraud-risk management obligations:

- Corporate agents and intermediaries must certify that they maintain their own fraud risk management framework commensurate with their business profile in line with the relevant IRDAI regulation.
- Individual agents must certify compliance with Aviva India's Anti-Fraud Policy.
- Promptly notify Aviva India of any suspected fraud involving Aviva India products or customers.

9. Training, Education and Awareness

9.1 Employee and Senior Management

Aviva India shall ensure that all employees and senior management receive comprehensive and proportionate fraud risk training in alignment with regulatory expectations. The training framework includes:

- Mandatory induction training for all new joiners covering Business Ethics and core Financial Crime topics, including fraud.
- Annual mandatory training for all employees on business ethics, fraud prevention, and Speak Up awareness.
- Enhanced, role specific training for functions exposed to heightened fraud risk—such as the Risk Control Unit (RCU), Claims, Underwriting, and Sales—to ensure deeper awareness of red flag indicators, prevention controls, and reporting obligations.
- Ongoing awareness and communication, including periodic email bulletins, e-learning materials, and leadership messaging to reinforce compliance expectations and emerging fraud risk themes across the organisation.

9.2 Third parties

Awareness programmes shall be conducted for policyholders, agents, and the public in accordance with IRDAI requirements. These programmes shall include the dissemination of information through periodic updates on Aviva India's official website, authorised social-media channels, and other approved public-communication platforms, with the objective of enhancing awareness of fraud risks and promoting responsible conduct across the insurance ecosystem.

10. Reporting Requirements

Aviva India, through the FMC, shall ensure timely and accurate reporting of fraud-related matters to the appropriate internal governance committees and external authorities, in accordance with regulatory obligations and the FRMF.

10.1 Internal

Through the FMC, Aviva India shall submit the following reports to the respective Board level committees:

- Quarterly Report to the RMC: A sufficiently comprehensive update on fraud risk management activities, key findings, emerging trends, recommendations, and the financial impact of fraud incidents.
- Annual FRA: A report of the annual fraud risk assessment, submitted to the Board through the RMC, outlining the fraud risk profile, control effectiveness and recommended strengthening measures.
- Internal fraud reporting to the Audit Committee: All internal frauds shall be reported to the Audit Committee, in addition to reporting through the RMC.

10.2 External

Aviva India shall comply with all regulatory and statutory reporting requirements relating to fraud, including:

- Annual filing with IRDAI: Submission of the annual fraud return in Form FMR 1 within 30 days of the close of the financial year, or within such timelines as may be prescribed.
- Immediate reporting of Distribution Channel fraud to IRDAI: Any fraud committed by distribution channels registered with IRDAI shall be promptly escalated and reported to the IRDAI without delay.
- Ad hoc reports to regulators or authorities: Any additional fraud related reports requested by regulatory or statutory authorities shall be prepared by the GI team and submitted through the Compliance function as appropriate.
- Reporting to law enforcement and other agencies: Aviva India shall report fraud cases, or provide information, to law enforcement or statutory authorities in accordance with applicable laws. Coordination responsibilities include:
    - Responding to law enforcement enquiries relating to frauds detected by Aviva India or reported to the Aviva India by the IRDAI.
    - Providing policy related information or records requested by statutory bodies such as CBI, Tax authorities, or other competent agencies.

11. Investigation Protocol

Aviva India has established documented investigation procedures and assigned clear responsibilities for each fraud category. The investigation of fraud is undertaken in accordance with approved SOPs (or equivalent procedural documents) and is allocated to the appropriate function/team.

For affinity/complex or collusion frau, on a case-by-case basis, and considering the specific circumstances of each matter, the relevant functions will confer to determine which function/team is best placed to lead the investigation and what support, if any, is required from other functions/teams.

12. Information Sharing & Coordination

In support of IRDAI's goal of an industry-wide intelligence network to combat fraud, Aviva India is committed to sharing fraud-related information as appropriate and in line with legal requirements with:

- IRDAI.
- Insurance Information Bureau (IIB).
- Life and General Insurance Councils.
- Other insurers (as applicable under regulation).
- Law-enforcement agencies.

13. Policy Review

This policy shall be reviewed at least annually, or earlier if required due to regulatory changes, emerging fraud risks or business developments.

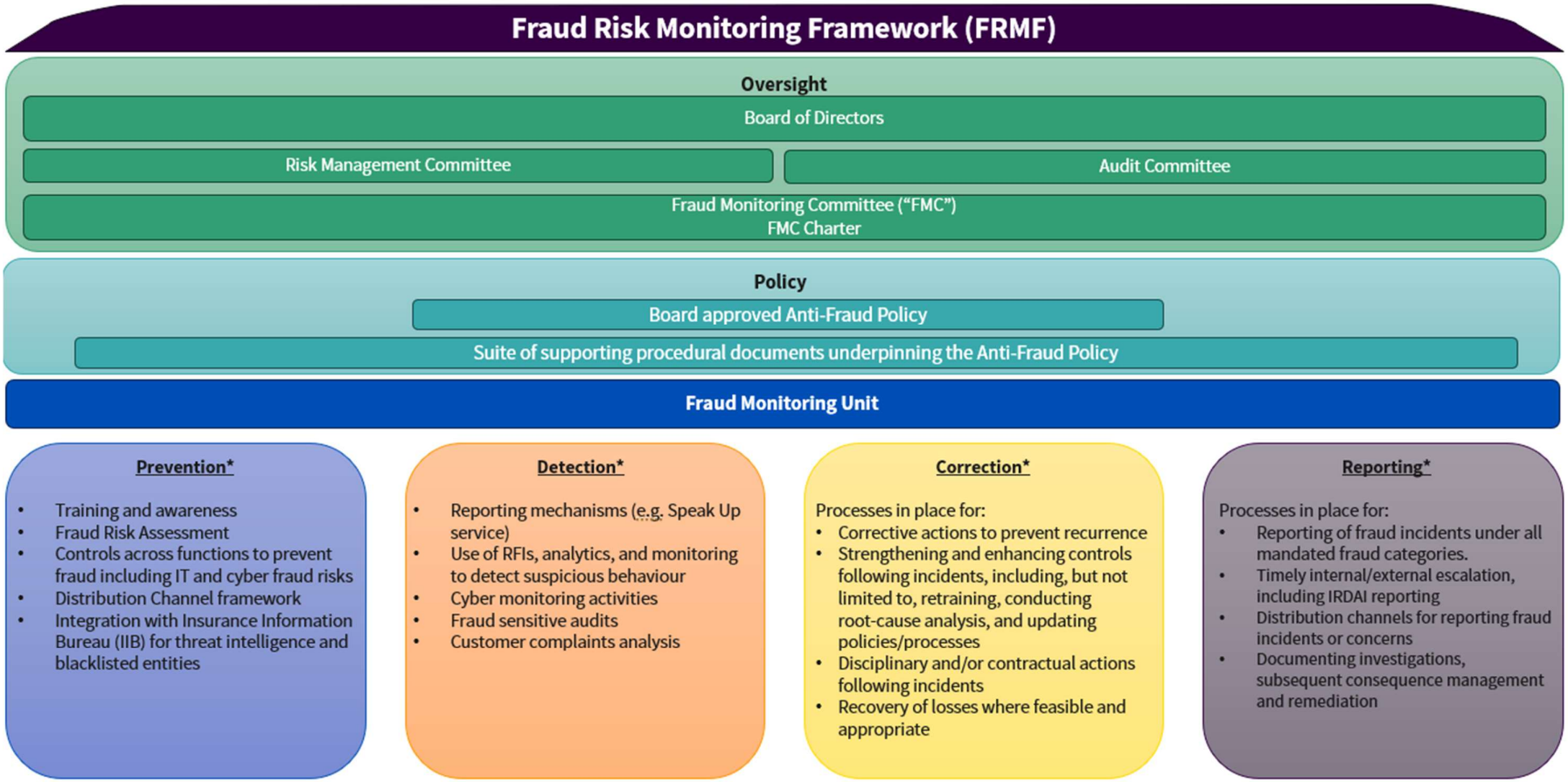
14. Annexures

- Annexure 1 — List of key supporting documents underpins this policy
- Annexure 2 - A high-level overview of the FRMF
- Annexure 3 - Examples of actions constituting fraud, RFIs, and Aviva India controls

Annexure 1 - List of key supporting documents underpins this policy

IRDAI requirement	Mapped documents to IRDAI requirements
Board-approved Anti-Fraud Policy + annual review + RFIs	Anti-Fraud Policy; FRA Methodology; Monitoring & Analytics Protocols/SOPs
Fraud Monitoring Committee (FMC)	FMC Charter; Anti-Fraud Policy
Fraud Monitoring Unit (FMU)	Investigations Charters/SOPs, FMC Charter; Anti-Fraud Policy
IRDAI taxonomy of fraud	Anti-Fraud Policy; FRA Methodology
IIB integration	Anti-Fraud Policy; Analytics Protocols/SOPs
Zero-Tolerance stance	Anti-Fraud Policy; Aviva's Business Ethics Code
Distribution channel framework	Distribution Channel SOPs/procedural documentation; Anti-Fraud Policy
IRDAI fraud reporting	Anti-Fraud Policy; Investigation Charters/SOPs
Cyber / New-Age Fraud controls	Cyber Security framework; Anti-Fraud Policy
Red Flag Indicators	Anti-Fraud Policy; FRA Methodology; RFI SOP
Full fraud lifecycle documentation	Investigations Charters

Annexure 2 - A high-level overview of the FRMF



** List of controls shown are for illustrative purposes and are not exhaustive.*

Annexure 3 - Examples of actions constituting fraud, RFIs and Aviva India fraud controls

Based on the nature, size, and distribution of Aviva India, the following provides an illustrative list of potential fraud, RFIs, and Aviva India fraud controls. This list is not exhaustive, and further examples can be found in the relevant supporting procedural documentation and systems.

IRDAI Category	Illustrative examples	RFI examples	Fraud control examples
Internal Fraud	• Misappropriation of funds or assets; improper handling/reporting of financial transactions • Forgery/alteration of company documents, checks, or financial records • Fraudulent alteration/addition/removal of information in MIS/systems • Fraudulent financial reporting • Granting special privileges or vendor favouritism/kickbacks • Inflating/overbilling expenses; paying false or inflated invoices • Removing/diverting money from customer accounts • Forging signatures or documents	• Employee overrides system controls frequently without reasonable explanation • Manipulation of customer records or backdating of transactions • Staff repeatedly involved in disputed claims, suspicious payouts, or policy alterations • Conflict-of-interest indicators (e.g., employee relationship with beneficiary or agent not disclosed)	• **Cash Misappropriation** ○ Systematic daily end of day cash reconciliation. ○ Disciplinary action for negligence or failure to report cash receipts. • **Forgery of documents (where internal handling/verification applies)** ○ Pre and post issuance document checks by branch operations for authenticity and completeness. ○ Mandatory customer signature verification by branch operations and processing teams. ○ PAN authentication (and OSV where applicable) for post sales service requests.

IRDAI Category	Illustrative examples	RFI examples	Fraud control examples
Distribution Channel Fraud	• Premium diversion (agent takes premium and fails to remit) • Premium inflation (collects more than due, remits correct amount, keeps difference) • Commission fraud (non-existent policyholders; first premium paid to trigger commission then lapse) • Mis selling (leading to refunds/rebates; churning/splitting policies) • Posting renewal premium as new business; fraudulent surrender of existing policies • Manipulation of proposal/OSV/medical documents; influencing doctors or using dummy applicants • Accepting/soliciting items of material value in exchange for undue advantage	• Agent involved in unusually high early-claim cases • High volume of similar-pattern proposals sourced from a single intermediary • Mis-selling-related complaints linked repeatedly to one advisor • Agent submitting documents that appear forged or inconsistent • Premium paid in cash repeatedly through same intermediary rather than customer-initiated payment routes	• **Mis selling** ○ PIVC (live video) confirmation of personal details and policy benefits to mitigate mis-selling. ○ Lessons learned from legal cases & grievances embedded into process improvements. ○ Root-cause analysis of complaints to identify trends; implement corrective & proactive actions.
Policyholder / Claims Fraud	• Underwriting fraud (deliberate misrepresentation/non-disclosure at inception) • Claims fraud (death/CI/waiver/PHI submitted when event didn't occur; staged/contrived events) • Medical claims fraud; reporting fictitious damage/loss (where applicable) • Policyholder impersonation; signature forgery by/for the insured • Assignment abuse (assigning policy to parties without insurable interest for value) • Proposal/claims documents for non-existent persons or where person was deceased pre-proposal • Same address/phone reused across unrelated customers (synthetic relationships)	• Proposal form contains inconsistencies, overwriting, or altered documentation • Insured dies shortly after policy issuance (early-death claims) • Multiple policies taken within a short period by the same life assured • Contact information (phone/email/address) appears invalid, fabricated, or belongs to an unrelated third party • Medical reports appear tampered with, inconsistent with age, occupation or known medical history • Beneficiary makes aggressive, urgent, or unusual attempts to expedite claim settlement • Claimant unable to provide basic documentation or provides conflicting statements	• **Surrender / Maturity fraud** ○ Payout request & KYC verification by branch operations for authenticity and completeness. ○ Mandatory signature verification for processing. ○ Disciplinary action for negligent/incorrect processing. • **Claims Fraud** ○ Early claims data shared with UW & RCU to analyse products, locations, customer profiles; feed red flags into new business controls. ○ System embedded red flags at NB → additional probing (financial/medical/physical/third party verification); pre issuance

IRDAI Category	Illustrative examples	RFI examples	Fraud control examples
		• Suspicious hospital/doctor with history of irregular claims	risk focused visits to validate socio economic profile. ○ Post issuance checks using IIB/industry flags; terminate negative policies pre claim where warranted. ○ Industry participation (AICM/AIU) and training to keep risk assessment current. ○ Investigation grid at death claim stage based on policy duration / sum assured; industry feedback used in decisions. ○ Participation in IIB fraud repository to avoid repeat industry fraud cases. ○ Escalation of suspicious cases (esp. with employee/agent involvement) to GI & Sales Compliance teams as appropriate for investigation.

IRDAI Category	Illustrative examples	RFI examples	Fraud control examples
External Fraud	• Application/identity fraud using third-party details • Pseudocode (fake death to claim benefits) • Phony policy fraud (fake policies sold by non-authorised actors) • Forgery by family/third parties to access policy details or benefits • Payments to fictitious suppliers; abuse of brand (impersonating insurer) • False statements to law enforcement/regulators (to obstruct or mislead)	• Suspicious patterns associated with third-party medical examiners or labs • Vendor invoices inconsistent with contracted rates • Collusion indicators such as repeated association between same doctor and fraudulent claims	• **Hoax / Spurious Calls** ○ Quarterly spurious-call awareness drives for customers. ○ Clear reporting pathways for customers to report such calls. • **Forgery of documents (when originating outside the firm, e.g., counterfeit KYC/medical)** ○ Pre- and post-issuance authenticity checks, signature verification, and PAN/OSV validation serve as safeguards against forged submissions by external parties.
Cyber / New-Age Fraud	• Phishing/vishing/social engineering to obtain policyholder credentials or divert payouts • Account takeover to redirect surrender/claim proceeds • Digital document tampering (e-KYC, medicals, OSV images) and device/identity spoofing • Spurious calling/scam campaigns impersonating the insurer • Data exfiltration/disclosure of confidential or proprietary information	• Multiple login attempts to customer portal from unusual geographies • Sudden change in beneficiary or bank details initiated digitally • Phishing-type communications sent to customers pretending to be from Aviva India • Policy alterations performed through compromised credentials	• System-embedded red flags • DLP • Information security policy and acceptable use policy along with training and awareness in this regard. • Escalation to GI for investigation with a defined investigation grid – supports coordinated handling of multi-actor cases. • Awareness to employees and customer to beware of cyber frauds • Industry collaboration (AICM/AIU) & IIB repository participation – improves intelligence-sharing and detection of wider networks.

Version Control

Version	Date	Author/editor/reviewer	Change description / comments
2013.01 (May 2013)	May 2013		
2014.02 (Aug 2014)	19-Jan-26		
2015.01 (Sep 2015)	Sep 2015		
Ver.2.0/AFP/082016	Aug 2016		
Ver. 3.0/AFP/10212016	21-Oct-16		
Ver. 3.1/AFP/17052017	17-May-17		
Ver. 3.2/AFP/16052018	16-May-18		
Ver. 3.3/AFP/12.12.2018	12-Dec-18		
Ver. 4.0/AFP/20.01.2020	20-Jan-20		
Ver. 4.1/AFP/31.03.2021	31-Mar-21		
Ver. 4.2/AFP/14.01.2022	14-Jan-22		
Ver. 4.3/AFP/16.05.2023	16-May-23		
Ver. 4.4/AFP/23.05.2025	23-May-25		
Ver. 4.5/AFP/15.01.2025	15-Jan-25		
Ver. 5.0_Feb2026	Jan/Feb 2026	Neeraj Jha (DVP, Group Investigations, Aviva India)	Updated in reference to the IRDAI IFMF 2025 guidelines Processed reviewer comments and updates
Ver. 5.0_Feb2026	9-13 Feb-26	Helen Anthony (Head of Investigations, Group Investigations, Aviva plc)	Inserted into current Aviva branded template. Reviewed and rewritten to align better the sections and content with the Guidelines, remove duplication, use consistent terminology, clear definitions, and move certain non-policy content to the relevant supporting documentation. Review and approval prior to review and approval by the FMC
Ver. 5.0_Feb2026		FMC members	Reviewed and approved at the FMC meeting dated 24th February 2026
Ver. 5.0_March 2026 (Revised Policy is effective from 1st April 2026)		Aviva India Board	Board approval - vide Circular Resolution no. 339 dated 1st April 2026

*A version change of X.0 denotes there have been material changes, which require Board sign off and evidence of FMC consultation as appropriate. A version change of 0.X denotes there have been non-material changes, which can be signed off by the policy owner with evidence that the FMC has been informed.

This policy shall be reviewed and approved at least annually, or earlier if required due to regulatory changes, emerging fraud risks or business developments.

"This Policy is as per applicable extant regulations/laws."