

Financial Crime

1 Policy objective

- 1.1 The objective of this policy is to provide the minimum standards for financial crime management for the Aviva group. Aviva is committed to minimising financial crime, which encompasses money laundering, fraud, malpractice and market abuse, and promotes a zero tolerance approach to financial crime.
- 1.2 Money laundering and fraud are key themes for the Financial Services Authority (FSA) and many other regulators worldwide. Most jurisdictions have amended their legislation to include the 'financing of terrorism' as part of their laws and regulations. Financial crime continues to be a high priority for governments and, consequently, provides continued reputational and legal risk to the group. In addition to the very visible financial losses and reputational damage caused by financial crime, any failure to establish adequate controls leaves the group and approved persons open to criminal sanctions including heavy fines.
- 1.3 The group strives to maintain the highest standards of governance, personal and corporate ethics, compliance with all laws and regulations and values integrity and honesty on dealings with all employees, customers, suppliers and other stakeholders.
- 1.4 Aviva is committed to supporting government, law enforcement and international bodies to combat the use of the financial services sector to facilitate financial crime.
- 1.5 Any breach of this policy may lead to reputational damage.

2 Policy owner

- 2.1 The group policy owner for this policy is the director of group financial crime.
- 2.2 The executive sponsor for this policy is the group finance director.

3 Primary audience

- 3.1 This policy provides direction to all staff on their roles and responsibilities in effectively managing financial crime. It should be communicated to all staff.

4 Scope

- 4.1 The scope of this policy is groupwide and applies to all Aviva operations including businesses and legal entities.
- 4.2 For joint ventures and outsourcing arrangements, senior management should satisfy itself, as far as reasonably practicable, that the systems and controls which are in place are appropriate to monitor and mitigate risk.

5 Alignment to risk appetite

5.1 Inherent risks

This policy supports management of the following inherent risks:

5.1.1 Money laundering

- The organisation is used as a conduit for the proceeds of crime or to facilitate the funding of terrorist acts.

5.1.2 Internal financial crime

- That acts of fraud, malpractice, corruption and / or any other illegal activities are undertaken by any employee.

5.1.3 External financial crime

- Failure to prevent or deter any act of fraud, malpractice, corruption and / or any other illegal activity that may be undertaken by an external party, this excludes policyholder fraud which is managed as part of business operations.

5.1.4 Regulatory and legal requirements

- Failure to ensure that there are appropriate systems and controls to manage financial crime risks which meet the requirements of regulators and legislators and could expose Aviva to regulatory or legal censure.

5.1.5 Market abuse

- Where external stakeholders have been unreasonably disadvantaged, directly or indirectly by others who have used information which is not publicly available or have distorted the price setting mechanism of financial instruments or have disseminated false or misleading information.

5.2 Risk appetite

In addition to the risk appetite statements specified in the risk management and internal control policy, the specific risk appetite statements in relation to this policy are as below.

The group has no appetite for:

- Incurring regulatory or legal censure, fines or prosecution relating to money laundering by failing to ensure our businesses comply with the laws and regulations of every country or territory in which Aviva operates.
- Failing to maintain a proportionate system of **internal controls** to prevent fraud, malpractice, corruption and / or any other illegal activity which may impact upon direct costs, our reputation, supervisory risk, ethics and customer care.
- Failing to maintain a proportionate system of controls to prevent fraud, malpractice, corruption and / or any other illegal activity from **external parties** which may impact upon direct costs, our reputation, supervisory risk, ethics and customer care.
- Failure of any part of the organisation to adhere to laws and regulations of the country or territory in which they operate. Also failure to implement the group anti money laundering or fraud and malpractice standards.
- Any form of behaviour which may constitute an offence of market abuse including the unauthorised release of price sensitive information.

6 Minimum standards

6.1 Risk management and control

The key risk processes and principles covering the inherent risk areas above are set out in this section.

6.1.1 Planning / change

Management information for financial crime risk should be used to provide insight and inform the operational planning process and influence resource allocation including capital.

6.1.2 Risk appetite

Risk appetite statements and tolerances should be clearly defined and refreshed on a regular basis (at least annually) and as an integral part of the planning process. Risk appetite should be defined for a business as usual situation within an established business and also needs to be sufficiently flexible to deal with a variety of situations (e.g. rapid market expansion, managing significant change) and should support rather than constrain sensible risk taking to deliver business strategy.

6.1.3 Risk analysis

Regular reviews (at least on a quarterly basis) of financial crime systems and processes must be actively performed to ensure inherent risks are effectively managed.

- i. Investigations - any investigation must be subject to regular review and oversight.
- ii. Pro-active financial crime detection - each business must regularly review their systems and process to identify instances of fraud or money laundering. Money laundering systems must be subject to risk based monitoring.
- iii. Prevention - risk assessments for fraud and money laundering must be maintained and updated regularly. Each business must have a completed fraud risk map and implemented effective controls to manage the risks identified.

6.1.4 Controls

Appropriate controls must be in place to ensure the following requirements are met:

Anti-money laundering

A. Documented procedures

- i. Documented procedures and controls that are compliant with this policy and the group AML standards must be in place. Additionally these procedures and controls must be compliant with local law and regulations. Arrangements must be in place locally and at group level to monitor compliance with the policy and standards.

B. Customer identification

- i. Reasonable steps must be taken to verify the identity of all customers. This will also include the beneficial owners of corporate entities (including trusts and other forms of entity using the products and services of Aviva) and any principals behind customers who are acting as agents.
- ii. Reasonable steps must be taken to ensure that "know your customer" (KYC) information is collected and kept up-to-date as far as practicable and that identification information is updated when changes occur to the parties involved in a relationship.
- iii. The level of KYC information collected will be in line with the risk based approach as set out in the standards.

C. Training staff

- i. Relevant staff must be trained on identifying money laundering, the recognition of suspicious activity, the requirements of local legislation and regulation, the group's policy and standards on anti-money laundering, and the procedures and controls for anti-money laundering. All staff must have access to information covering their

legal and regulatory responsibilities in relation to anti-money laundering.

D. Support government and international bodies

- i. Governments, law enforcement agencies and international bodies must be supported in their efforts to combat the use of the financial service industry for the laundering of the proceeds of crime or the movement of funds for criminal purposes.

E. Maintain records

- i. Procedures must be established to retain all relevant records (e.g. customer identification, policy opening documents) for a minimum of five years (unless local regulations stipulate a longer period). These records must be retained for five years after a relationship has ended. Records relating to training, compliance monitoring and any internal and external suspicious activity reports should also be retained for a minimum of five years.

Fraud management and malpractice reporting

A. Training staff

- i. Fraud training and awareness must be undertaken by all members of staff.

B. Culture and ethics

- i. All reasonable steps must be taken to ensure that the culture and ethics within individual businesses reflect the Aviva values and must promote a zero tolerance approach to financial crime.

6.1.5 Actions

Where differences in risk appetite and the residual risk profile have been identified by the risk analysis process, remedial action plans must be put in place. In instances where controls are deemed to be deficient, these action plans should include improvements in both the control design and its operation. In all cases action plans should contain SMART (specific, measurable, achievable, realistic and time-bound) actions with progress reported on a regular basis to management.

A. Investigations

- i. A documented fraud response plan must be in place which clearly details how fraud will be reported and investigated within individual businesses.
- ii. All investigations must be carried out objectively and confidentially.
- iii. The investigation must be independent of the line management for the area in which the fraud is suspected.

B. Post investigation actions including external reporting

- i. All cases of fraud or malpractice must be reported to local law enforcement, and where required locally, to regulatory bodies or government agencies.
- ii. The recovery of monies lost due to fraud should be actively pursued using available legal means where appropriate.

6.1.6 Line management and reporting

Anti-money laundering

A. Identification of suspicious activity

- i. Procedures must be established to ensure that reports of suspicious activity or suspicious proposed activity (including business not taken on due to suspicion) are reported through the appropriate internal channels and, where required, to any relevant external authorities. Additionally, co-operation will be given to any lawful request by government agencies to assist in money laundering investigations.

B. Reporting

- i. Procedures must be in place to enable the reporting of money laundering issues to local senior management and group senior management on a regular basis. The group money laundering reporting officer (GMLRO) will determine and communicate the content, format and frequency of management reporting, in conjunction with business money laundering reporting officers (BMLROs).

C. Internal accountability and responsibility

- i. Clear lines of internal accountability, responsibility and reporting must be established.
- ii. Primary responsibility for the prevention of money laundering rests with the head of each business.
- iii. Appropriate internal controls must be in place, operating effectively and staff must be adequately trained.
- iv. The head of each business is required to appoint a business money laundering reporting officer (BMLRO) who is responsible for ensuring the business complies with the standards. This will be supported by the group money laundering reporting officer (GMLRO), who will be responsible for the ownership of group policy and the production of group anti-money laundering standards.

Fraud management and malpractice reporting

A. Internal reporting

- i. Procedures must be in place in each business to enable the reporting of fraud and malpractice incidences to local senior management and group senior management on a regular basis. Significant frauds as defined by the standards must be escalated to the group director of financial crime. The director of financial crime will determine and communicate the content, format and frequency of management reporting, in conjunction with business policy owner.

B. Malpractice reporting

- i. A safe mechanism must be provided for management and staff to report without fear, suspicions of fraud, theft and malpractice, while guaranteeing anonymity when requested.
- ii. Suspicions of fraud, theft and malpractice must be investigated independently using best practice investigation techniques as set out in the fraud and malpractice standards.

C. Internal accountability, responsibility and resourcing

- i. Clear lines of internal accountability and responsibility for the prevention, detection and investigation of fraud and malpractice

must be established and sufficient resource must be available to meet these requirements.

Escalation of breaches

- i. All breaches of this policy, including any identified issues that could lead to a breach, should be notified to the group policy owner and the regional chief risk officer immediately (within 24 hours). Where breaches are identified that are material at group level, the group chief risk officer should also be notified.
- ii. Materiality of a breach or issue can be determined by reference to the delegated authority limits for risk management that outline the relevant escalation protocols.
- iii. The group policy owner will advise the relevant oversight committee (e.g. ORC or ALCO) and executive sponsor of all material breaches.
- iv. As primary responsibility for risk management lies with line management it is expected that breaches will be also reported up through functional management. All breaches should be documented through the quarterly risk reporting cycle.

6.2 Responsibilities

6.2.1 Business

Head of business:

- Ensures that the business manages financial crime risk and operates in line with the minimum standards in this policy.
- Maintains an appropriate control structure and culture to manage financial crime risk exposure within appetite.
- Meets management information reporting requirements to demonstrate that financial crime risks within the business are being managed effectively.
- Has ultimate responsibility and accountability for financial crime within their jurisdiction. They must ensure that prompt action is taken to resolve any financial crime issues which are deemed to be unacceptable. Such issues must also be escalated to the director of financial crime in line with the escalation process contained in the standards.
- The head of business must appoint a local policy owner to be responsible for ensuring compliance with this policy and the group fraud and anti money laundering standards. The local policy owner must be of sufficient seniority in the business and possess the requisite skill and experience necessary to ensure effective management of the policy.

Local policy owner:

- Acts as a local subject matter expert and provides guidance in relation to the policy.
- Ensures that the requirements within this policy are understood by the business to assist them in implementing local compliance monitoring arrangements.
- A set of standards has been created which detail the anti-money laundering and fraud and malpractice management requirements separately. Individual businesses are required to comply with these standards. It is the local policy owner's responsibility to ensure that the standards are complied with and that there is sufficient resource to enable the implementation of the policy and the standards. Businesses

must incorporate these responsibilities within the policy owner's job description, objectives and performance assessments.

6.2.2 Region

The responsibility of the region is to provide appropriate oversight and challenge, as part of the second line of defence, in order to satisfy itself that the businesses in the region operate in line with this policy.

6.2.3 Group

Group policy owner:

- Maintains the integrity of policy content and develops adequate guidance material to support implementation.
- Acts in an advisory capacity to set the risk appetite and provides guidance on establishing the control environment to ensure risks are managed within appetite.
- Provides advice, support and technical guidance in relation to the policy, including application for waivers and notification of breaches.
- Defines the management information required from the business for the oversight committees to discharge their governance oversight and also provides technical advice and reports to these committees as appropriate.
- Provides a report to the audit committee at least on a quarterly basis. Each year an annual report is presented to the group risk and regulatory committee.

Other responsibilities:

- Where there is reasonable suspicion that fraud or malpractice has occurred anywhere within the group, group financial crime or the group policy owner is entitled to investigate the suspicions thoroughly using recognised and legitimate investigation techniques.
- The director of financial crime is authorised to enter any group premises, be given access to any information requested and have access to all staff. This right of access can be delegated to any member of group financial crime at the discretion of the director of financial crime.

6.2.4 Staff

It is the responsibility of all staff to report their suspicions of financial crime as set out in this policy.

7 Waivers and exceptions

- 7.1 In exceptional circumstances, and on a case by case basis, a waiver or exception may be granted to this policy.
- 7.2 All requests for a waiver or exception in respect of any requirements of this policy must be discussed with the regional chief risk officer. Applications should be forwarded to the group policy owner (cc group chief risk officer) with a supporting detailed business / operational justification signed by the business head requesting the waiver or exception.
- 7.3 The group policy owner, in liaison with the group chief risk officer, will decide upon the application and advise the region of the outcome. The group policy owner will provide details to the relevant oversight committee (i.e. ORC or ALCO) and executive sponsor of any waivers or exceptions granted.

8 Reference to supporting materials

8.1 Group financial crime standards

This policy and the supporting standards set out the detailed processes and procedures necessary for effective financial crime risk management across the group.

This policy forms part of the group's overall approach to the management of financial crime. The associated group policies listed below should also be taken into consideration as part of the overall approach to mitigating the risk of financial crime:

- corporate social responsibility
- regulatory risk
- legal risk

8.2 Group committees

Terms of reference are available on the intranet for the group committee mentioned in this policy:

- Group Audit Committee (GAC)

8.3 Risk and control matrix

This document demonstrates the linkage between the inherent risks, control objectives, and illustrative key controls and key indicators (qualitative and quantitative) that can be used to provide insight and evidence as to whether the inherent risks the policy is seeking to address are being mitigated adequately in practice.

A matrix should be maintained for each policy. Gathering evidence through indicators will provide the insight into the effectiveness of the internal control environment, and so limiting the need for detailed testing.

8.4 Glossary

A central glossary is maintained within the risk management and internal control policy. There are no specific terms unique to this policy so no technical glossary is provided.