

FINANCIAL CRIME RISK MANAGEMENT POLICY

Contents

1. PURPOSE OF THE POLICY	3
2. APPLICATION OF THIS POLICY	3
3. FINANCIAL CRIME RISK MANAGEMENT VISION AND MISSION	4
4. FINANCIAL CRIME RISK APPETITE STATEMENT	4
5. POLICY FORMULATION	5
6. ROLES AND RESPONSIBILITIES	5
7. FINANCIAL CRIME RISK MANAGEMENT MANDATE	5
8. FINANCIAL CRIME RISK MANAGEMENT OPERATING MODEL	6
9. REPORTING SUSPICIONS OF FINANCIAL CRIME	9
10. BREACH OF POLICY	10
11. REPORTING	10
12. AMENDMENTS TO THE POLICY	10
13. POLICY ADMINISTRATION	10

1. PURPOSE OF THE POLICY

This document defines the Financial Crime Risk Management (FCRM) Policy for Hollard Holdings (HH), The Hollard Insurance Company (THIC), Hollard Life Assurance Company (HLAC), Hollard Specialist Insurance (HSI) and Hollard Specialist Life (HSL) (“Hollard”) and the regulated insurance entities operating within the Group.

Managing financial crime within Hollard requires a definitive strategy combined with a good value and ethics system. FCRM involves a number of measures which form part of a “layered” approach to mitigating financial crime risk. A best practice FCRM model has four key focus areas, namely; prevention and detection, investigations (response) and remediation, all underpinned by an effective governance model.

The purpose of this Policy is to:

- Set out the principles for the management of risk and compliance associated with financial crime (internal and external), including, money laundering, terrorist financing, bribery and corruption, within Hollard;
- Provide a framework within which financial crime will be addressed in Hollard, to give effect to the Prudential Standard on Governance of insurance 3 (GOI 3) Risk Management and Internal Controls;
- Set the “Tone from the Top” of FCRM with a clear statement from the Board and Executive Management (“Exco”);
- Outline the principles and strategy of the prevention, detection, investigation, remediation and governance of financial crime and the effectiveness thereof within Hollard;
- Socialise the reporting obligations in terms of the Prevention and Combatting of Corrupt Activities Act (PRECCA) and make provision for the confidential and anonymous reporting of financial crime in terms of the Protected Disclosures Act; and
- Outline the mandate of the FCRM function of Hollard.

2. APPLICATION OF THIS POLICY

The requirements set out in this Policy apply to Hollard Holdings (HH), The Hollard Insurance Company (THIC), Hollard Life Assurance Company (HLAC), Hollard Specialist Insurance (HSI) and Hollard Specialist Life (HSL) and provides mandate for the Group and Business FCRM functions.

The implementation of this Policy will be proportionate to the nature, scale and complexity of each of the various Companies. The principle of proportionality is of particular importance to ensure the consistent application of the Policy whilst ensuring a fair and balanced approach to implementation. Proportionality is broadly defined with reference to the following measures:

- *Nature* – The specific nature of insurance activities including, for example, types of lines of business and the number of lines of business;
- *Scale* – The size of insurance activities including for example gross premium and maximum risk retention;
- *Complexity* – The complexity of the insurer and its activities including the business and distribution model, governance structures, product design, number of lines of business and special or alternative risk transfer activities.

This Policy applies to members of the Hollard Board, Executive and Senior management, Hollard employees, contractors, partners, customers, suppliers/ vendors, and intermediaries. Any agreement entered into with the aforementioned parties should include an express reference to the application of this Policy. Consequences of committing a Financial Crime could include the following:

- Disciplinary action which could result in dismissal;
- Termination of agreements or contracts;
- Reporting to the Financial Sector Conduct Authority (FSCA) which could result in debarment;
- Criminal case reporting including Prevention and Combating of Corrupt Activities (PRECCA) reporting where applicable in terms of the legislation;
- Civil case proceedings;
- Recovering of funds through the individuals Pension / Provident Fund and through Section 300 in terms of the Criminal Procedure Act; and
- Reporting to the relevant Regulatory Authorities and Insurance Industry Bodies such as the Insurance Crime Bureau.

Transparency is critical to the effective management of financial crime risks within Hollard. The repayment or any offer to repay misappropriated funds or the return of any object associated with the misconduct, or if an individual opts to leave Hollard's employment or cancel the contractual relationship, will not absolve responsibility and will not constitute exceptional mitigating circumstances for deviation of Hollard's commitment to the enforcement of consequence management in line with the 'no tolerance to financial crime' approach.

All persons involved in, or that assist with, conduct that falls within the definition of financial crime as contained in the Policy and all persons who are aware of misconduct and who fail to report it in accordance with the provisions of this Policy, shall be in breach of this Policy.

3. FINANCIAL CRIME RISK MANAGEMENT VISION AND MISSION

To provide Hollard and its stakeholders with Financial Crime Risk Management solutions in support of a "Green Control Environment" to mitigate financial crime exposure and minimise the impact thereof.

This will be achieved by providing strategic Financial Crime Risk Management solutions across the value chain (prevention, detection, investigations and remediation), underpinned by an effective governance model.

Financial Crime Risk Management – Partnering with all stakeholders to protect Hollard.

4. FINANCIAL CRIME RISK APPETITE STATEMENT

Hollard will avoid the risk of financial crime, which entails the risk of loss due to acts to defraud, misappropriate property or circumvent regulations, the law of company policy and harm Hollard or a third party.

Hollard will implement processes and controls that provide for reasonable and proportionate mitigation against internal and external financial crime. Hollard has no appetite for financial crime. Hollard accepts that

its operating environment creates exposure to the risk of internal and external financial crime. Internal or external practices that lead to, support, or enable financial crime are in direct contravention to Hollard’s purpose and values.

Hollard will mitigate financial crime risk through a combination of group wide initiatives including prevention, detection, investigations and remediation.

The management of financial crime risk is the accountability of the respective Business Unit and Centre function Executives. Business units will establish dedicated financial crime capabilities to proactively deliver on the above commitment through the design, implementation and monitoring of fit for purpose controls that support the delivery of business outcomes.

Hollard will establish a dedicated Group Financial Crime Risk Management capability (in support of the Group Risk Management control function) to execute its responsibilities including establishing a Financial Crime Risk Management Policy, independent monitoring of business activities, including oversight on Business Unit FCRM functions, conducting all Hollard staff investigations independently from business, expressing a view on financial crime risk and meeting Board and Regulatory reporting requirements.

5. POLICY FORMULATION

The principles and objectives of the Hollard FCRM Policy will be supported by several policies, standards, procedures and other documentation adopted throughout Hollard, as well as relevant legislation. This Policy must be read in conjunction with Hollard’s risk policies and all Hollard employment policies.

6. ROLES AND RESPONSIBILITIES

Financial crime risk is an operational risk and is defined in the ERM Framework with a key focus on internal and external financial crime risks that impact Hollard. The detailed risk management roles and responsibilities for key stakeholders in Hollard’s system of risk management are outlined in the ERM Framework. These include the minimum regulatory requirements as prescribed by regulators. Practical application and additional details about Hollard’s risk operating processes as it relates to the Board, Senior Management, Control Functions and Combined Assurance are set out in a number of stand-alone policies.

The Group FCRM function operates within the Risk Management function and primarily serves the role as the “2nd line of defence” within the system of risk management. The Business FCRM function or equivalent function set up in business operates within the “1st line of defence” under the “business assurance” function or equivalent function set up to support the Senior Management of the business to maintain a system of internal control relating to financial crime risks.

The detailed roles and responsibilities for the Group FCRM function as well as the Business FCRM functions have been outlined in the FCRM Engagement Model and point 8 of this policy.

7. FINANCIAL CRIME RISK MANAGEMENT MANDATE

The Group FCRM and Business FCRM functions receive its mandate from the Audit and Compliance Committee as delegated by the Board, in terms of this Policy.

The Group FCRM function must have seniority and authority, have reporting lines that support independence, unrestricted access to relevant information, direct access to the Board through the powers attached to the Chief Risk Officer (CRO), freedom to report to the Board without fear of retaliation from Senior Management.

The FCRM function has the authority to examine, copy and / or remove all or any portion of the contents of files, desks, cabinets, and other storage facilities, including electronic storage devices, on Hollard premises or intellectual property of Hollard, without prior knowledge or consent of any individual who may use or have custody of any such items or facilities if it is within the reasonable scope of their investigation and within legal limits of the country's laws and other company policies.

During the execution of financial crime risk management activities, FCRM shall obtain the necessary assistance from staff and management of Hollard as well as from other specialised services from within and outside the Group, within the prescriptions of this Policy, or as approved from time to time by the Head of the Group FCRM function or the CRO.

The FCRM team mandate extends to the following financial crime risks (perpetrated either internally or by external parties) against Hollard, but is not limited to:

- Any dishonest or fraudulent act;
- All matters that may have potential staff involvement;
- Misappropriation of funds, securities, supplies, or other assets;
- Impropriety in the handling or reporting of money or financial transactions;
- Profiteering as a result of insider knowledge of company assets;
- Disclosing confidential and proprietary information to outside parties;
- Disclosing to other persons, securities activities engaged in or contemplated by the company;
- Conflict of interest;
- Cyber related crime;
- Bribery and corruption;
- Money Laundering;
- Destruction, removal, or inappropriate use of records, furniture, fixtures, and equipment; and
- Any similar or related irregularity or non-adherence to related Hollard policies.

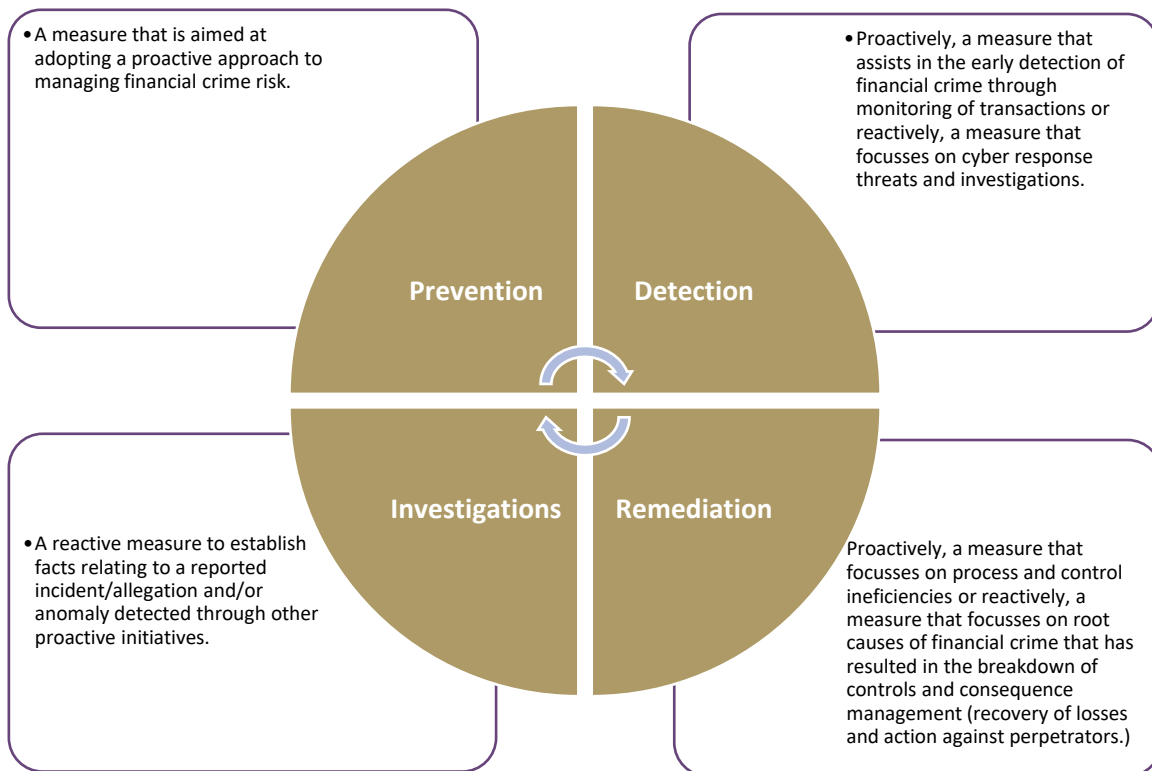
8. FINANCIAL CRIME RISK MANAGEMENT OPERATING MODEL

Hollard adopts an integrated and holistic approach to financial crime risk management, across the FCRM value chain and Hollard has no tolerance for financial crime.

The FCRM model is designed to ensure that objectivity and independence is maintained during execution of core components of the FCRM value chain.

The following diagram illustrates the core components of Hollard's system of financial crime risk management. The effective operation of these components is required in order to meet the principles and objectives set out in the FCRM strategy.

The FCRM value chain focuses on the following:



The FCRM model is developed on an integrated framework, with clear interdependencies within all specialisation areas within FCRM, supporting the strategic view that “the whole is more than the sum of its individual parts.”

The FCRM value chain focuses on the following:

a) **Prevention**

The key focus areas for financial crime risk prevention includes:

- *Financial crime risk awareness and training:*
Ongoing awareness and training promote a culture of good governance and increased vigilance regarding financial crime related risks. Awareness and training initiatives may include induction for new recruits, general financial crime awareness and policy training, red-flag and document fraud training and process and control training.
- *Financial crime risk marketing and communications:*
Effective marketing and communications support the strategy of FCRM by encouraging vigilance and reporting of financial crime within Hollard.
- *Financial Crime Risk Assessments and Combined Assurance Reviews*
A risk-based approach is adopted in collaboration with business to assess the prevalent financial crime risks and associated controls. A root cause analysis and trends are conducted on financial crime loss

events with the objective of improving the control environment. Combined Assurance Reviews will be conducted in collaboration with other Assurance Providers within the Three Lines of Defence model.

b) Detection

The key focus areas for financial crime risk detection includes:

- *Financial Crime Data Analytics & Continuous Monitoring:*
It is critical that the FCRM function have a monitoring process in place to serve as an early detection control, highlighting potential financial crime. Exception reports must be developed on known financial crime scenarios which will highlight “red flags” to assist business to mitigate financial crime risk.
- *Financial Crime Reporting:*
An inclusive case administration system must be in place to ensure that accurate financial crime statistics are collated and reported across the financial crime risk management value chain. Reporting on financial crime statistics is prescribed for various industry and regulatory institutions.
- *Digital Forensics Framework and Services:*
As part of an effective detection strategy, an operative digital forensics framework will support the mitigation of threats in the electronic media utilised by Hollard. Digital forensic services are critical in examining electronic media for evidence required for the management of financial crime risks perpetrated against Hollard either internally or externally.

c) Investigations

The investigations’ function provides an end-to-end investigation service, through the identification and classification of financial crime risk types, in accordance with the approved methodology. Effective investigation outcomes support the consequence management process and minimises losses to Hollard.

Group FCRM will Investigate matters arising from Hollard’s Central Units, projects that identifies common risks across Hollard, and all internal investigations (staff investigations) across Hollard as well as any ad hoc investigations / projects assigned to Group FCRM for investigation by the Board, Sub Committees or Executive Committee (Exco).

Business FCRM functions will deal appropriately with all operational investigation matters, claims assessments, preliminary screening and investigations, excluding staff investigations. Where there is a suspicion of staff involvement in matters investigated by business, these must be referred to Group FCRM.

d) Remediation

The key focus areas of Remediation include:

- *Remedial Actions*

All control environment remedial actions that support a “green control environment” recommended to business in relation to financial crime risk and all consequence management (disciplinary action, regulatory action, criminal action, civil action and industry action) will be tracked, monitored and reported to ensure value add to Hollard.

9. REPORTING SUSPICIONS OF FINANCIAL CRIME

The FCRM function promotes the reporting of financial crime against Hollard.

Hollard subscribes to the Protected Disclosures Act (Act 26 of 2000) as amended, which encourages the reporting of all suspicions of financial crime to Hollard. All whistle-blowing reports are treated as either confidential or anonymous.

Confidential whistleblowing occurs when a whistle blower may choose to reveal his / her identity when making a disclosure. Hollard will respect and protect the confidentiality of the whistle blower and provides assurance that their identity will not be disclosed to any third party. The only exception to this assurance is if Hollard is ordered by a Court of Law to reveal confidential information relating to a whistleblowing report.

Whistleblowing reports may also be made anonymously, whereby the whistle blower may choose not to reveal their identity when making a disclosure. An Ethics tip-off line has been established to report suspicions of financial crime, non-compliance and unethical behaviour. The Ethics tip-off line is managed by an independent third party. Hollard uses the services of Deloitte and reports may be made to Hollard@tip-offs.com or 0801-516-170. Management of the Ethics tip-off line is guided by an established process which ensures that no potential conflicts of interest exists between the subjects implicated in the report and the recipient of that report.

Any employee, contractor, partner, vendor or intermediary who has a reasonable suspicion that financial crime is committed against Hollard has an obligation to report the matter, using the reporting mechanisms in place. Confidential reports may also be made directly to the FCRM functions.

All reports must be made without malice and in good faith. In cases where malicious disclosures are made, disciplinary action may be taken against internal parties or legal action may be taken by the affected party. Staff are obligated to report any suspected financial crime risks to FCRM and failure to do so may result in a disciplinary enquiry.

Hollard does not operate a formal policy for rewarding whistle blowers. Line management may however offer such reward in exceptional circumstances that leads to the protection of Hollard’s licences and/ or its stakeholders. Such a decision will be taken collaboratively with Executive management of the Risk functions and Senior management as defined in the ERM policy.

Any individual who reports or provides information as part of an investigation must maintain the confidentiality of the information and investigation. This is important to avoid damaging the reputation of individuals identified as persons of interest or subject of investigation, where substantiating evidence of such conduct has not yet been established and to protect Hollard from potential civil liability. Hollard reserves the right to publish details of any misconduct once the appropriate internal and/ or external consequence management processes and decisions have been ratified by the responsible Executive and/ or authorities.

10. BREACH OF POLICY

Lack of adherence to this Policy may have severe consequences to Hollard and its Employees including:

- violating Financial Crime laws and regulations
- receiving monetary fines, criminal penalties, and/or regulatory enforcement orders
- exposing Hollard to financial, customer, operational, legal and reputational risk.

A breach is defined as non-compliance with any requirement in this Policy or underlying directives which has not been approved by the administrator of this policy. The policy owner must assess any potential breach to this policy and report accordingly to Hollard Group Exco, relevant Board Sub-Committees and other external authorities.

Non-compliance with this Policy and its underlying directives may result in disciplinary action, which may include dismissal, contract termination, criminal prosecution, or a claim for damages.

11. REPORTING

The Head of Group FCRM shall report on financial crime risks, compliance with this Policy and any other related issues to Hollard Group committees or any other external industry and regulatory bodies.

12. AMENDMENTS TO THE POLICY

Any material amendments to the ERM framework and this Policy that shall affect its nature will be approved by the Board. All other amendments shall be approved by the Chief Risk Officer.

13. POLICY ADMINISTRATION

Policy Owner: Chief Risk Officer (CRO): Wikus Luus

Policy Administration: Group Head: Group Financial Crime Risk Management: Roshen Ganaspersad

Version Control:

Policy Name	Version	Approval Date
Financial Crime Risk Management (FCRM) Policy	3	February 2023

Frequency of Review	Date of Next Review	Date of Last Review
Every two years or as required	February 2025	July 2018