FRAUD AND CORRUPTION RISK MANAGEMENT PLAN

Type of policy:	Fraud and Corruption Risk Management Plan
Executive summary:	The scope of this policy is applicable to Constantia Risk and Insurance Holdings (Pty) Limited (CRIH) and its insurance subsidiaries including Constantia Life Limited (CLL). The policy sets out the obligations of the Board of Directors of CRIH and its subsidiaries to oversee the fitness and propriety of Key Individuals and its Significant Owners.
Area of governance:	Compliance, Legal and Risk
Approving authority:	The Board of Constantia Risk and Insurance Holdings (Pty) Limited
Group Exco sponsor:	CEO
Responsible department:	Enterprise Risk Management
Date of approval:	November 2024
Review frequency:	Annually
Date of next review:	November 2025
Version:	V4.0 (Four)
Draft resolution:	The Insurance companies within the Constantia Risk and Insurance Holdings (Pty) Ltd group of companies recognise the value as well as the risks associated with the Regulatory requirements pertaining to their activities. This policy statement and framework has been approved by the Board of Directors of each of the above listed insurers who have duly authorised the signatories to this document. The Board is required to approve the policy in line with regulations with specific reference to Governance and Operational Standards for Insurers (GOI 3 and GOI 5).

SIGNED AT Kyalami ON THE DAY 21 OF January 2025

Themba Baloyi
Themba Baloyi (Jan 21, 2025 15:24 GMT+2)

TP BALOYI
CHAIRPERSON OF THE BOARD
INDEPENDENT NON-EXECUTIVE

SIGNED AT Cape Town ON THE DAY 3rd OF December 2024

Lukani Mulaudzi (Dec 3, 2024 18:11 GMT+2)

LK MULAUDZI
CHAIRPERSON OF
THE JOINT AUDIT & RISK COMMITTEE
INDEPENDENT NON-EXECUTIVE

Table of Contents

1. **INTRODUCTION** **3**
2. **DEFINITIONS** **5**
3. **FRAUD PREVENTION METHODS** **5**
4. **MANAGING FRAUD, BRIBERY & CORRUPTION RISK** **8**
5. **ROLES AND RESPONSIBILITIES** **10**
6. **REPORTING OF FRAUD** **12**
7. **EVALUATION AND MONITORING OF THE FRAUD PREVENTION** **12**
8. **REVISION HISTORY** **13**

1. INTRODUCTION

1.1. In accordance with CRIH's Anti-Fraud and Corruption Policy, the Group must implement a Fraud Risk Management Plan to reduce the risk of fraud, bribery and corruption and where incidents do occur to ensure that they are properly investigated and managed in accordance with the policy.

1.2. The prevention plan must consider the following:

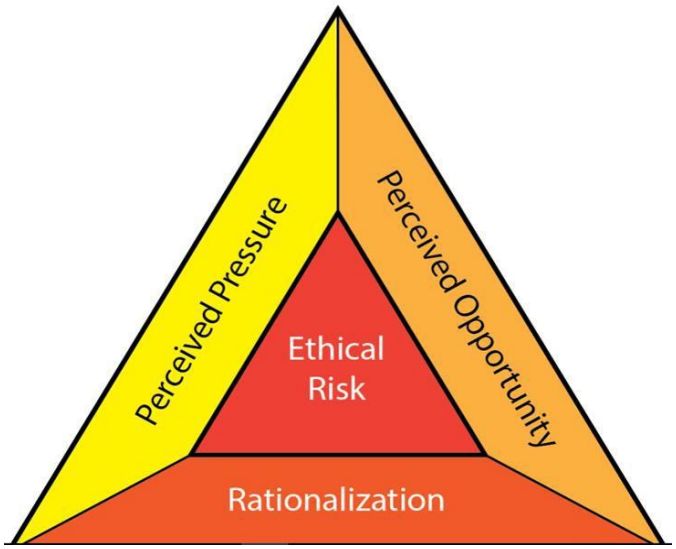
(a) a Risk Based Approach, considering the cost versus benefit;

(b) the Legislative environment in which the Group operates;

(c) learnings from its own and external fraud/corruption events; and

(d) the historical background to the Group, partners, and its associated companies.

1.3. Fraud and corruption arise from corrupt business practices that create unfair markets, erode public trust, and hinders growth. It is recognised that due to our business model and the complexity of our business, the issue of moral hazard driven by asymmetric information could result in breaches despite our efforts to strengthen rigorous application of our controls. This fact dictates that there should be a passive and an aggressive response that matches the substance of the illegal activity whilst dealing with the "soft, non-monetary and emotional aspects". To fully understand this, one must understand the "Fraud Triangle" and its basis. Refer to the figure below:



1.4. The unlawful and intentional making of a misrepresentation by staff (and others) is generally encouraged by some of the following factors:

1.4.1 Perceived Pressures

1.4.1.1 It is what motivates the crime in the first place, one is having financial troubles that he/she is unable to solve through legitimate means, so he/she begins to consider committing an illegal act:

(a) financial pressures;

(b) personal habits (gambling, drugs, alcohol);

(c) work-related factors (overworked, underpaid, not promoted);

(d) achieve financial results (bonus, compensation); and

(e) high debt level (encouraged by desires for status symbols such as bigger house or car).

1.4.2 Perceived Opportunities

1.4.2.1 It defines the method by which the crime can be committed. The person must see some way he can use (abuse) his position of trust to solve his financial problem, with a low perceived risk of getting caught. Such opportunities are created by:

(a) poor internal control (including no “4-eyes” principle);

(b) lack of segregation of duties where applicable;

(c) low fraud awareness;

(d) treatment of a fraudster with leniency;

(e) rapid turnover of employees;

(f) use of many Banks;

(g) weak subordinate personnel; and

(h) absence of mandatory vacations.

1.4.3 Rationalisation

1.4.3.1 A vast majority of fraudsters are first time offenders with no criminal past, they do not view themselves as criminals, they see themselves as ordinary and honest people who are caught in a bad circumstance, so they rationalise their behaviour, such as I am only borrowing the money and will pay it back:

(a) nobody will get hurt;

(b) the company treats me unfairly and owes me;

(c) it is for a good purpose; and

(d) it is only temporary, until operations improve.

1.5 The fraud risk prevention methods use two inter-related enablers to achieve the overall objective of fraud and corruption risk management (managing the unlawful and intentional making of a misrepresentation):

(a) Primary Enablers of established background activities that are non-intrusive, and

(b) Secondary enablers to Fraud and Corruption Prevention.

2. DEFINITIONS

2.1. **Bribery** means the offer/receipt of any kickback, gift, loan, fee, reward/other advantage to/from customers, agents, contractors, suppliers, intermediaries, or employees of any such party or to/from government officials, as an incentive to do something which is dishonest, illegal, improper, a breach of trust or a breach of the policy or principles for its employee's benefit or that of the employee's family, friends, or business associates.

2.2. **Corruption** means the offering, giving, soliciting or acceptance of an inducement or reward (including facilitation payments or hidden commissions) which may improperly influence the action of any person in relation to the business.

2.3. **Facilitation Payments** means the improper payments made to facilitate or expedite the performance of "routine" governmental action.

2.4. **Code of Conduct** means an agreement between the Group and its employees, specifying standards of behaviour expected. Employees agree to the code when they join the Group, and so agree to uphold its standards.

2.5. **Gifts/Hospitality** means items, goods, services, corporate entertainment, and business assistance from which the person giving or receiving the gift/hospitality may get benefit, and any other benefit or gratuity.

3. FRAUD PREVENTION METHODS

3.1. The Group has, over several years of operations, established a wide-ranging system of strategic and operational mechanisms/controls to deal with fraud and corruption risk prevention. These mechanisms/controls were/are designed to prevent, deter, and detect fraud and corruption daily and include:

(a) A system of Corporate Governance with a Board of Directors chaired by an independent Director with sub-committees for Audit, Risk and Remuneration functions. Most of the Board of Directors are independent and non-executive.

(b) Directors and all employees are informed and educated regarding their fiduciary duties and responsibilities towards the Group and all its stakeholders.

(c) An annual Strategic Plan document, which incorporate forward planning into a five-year period, approved by the Board of Directors with monitoring and reporting to the Board on a quarterly basis.

(d) A set of policies, procedures, systems, and internal controls approved by the Board of Directors.

(e) An integrated reporting framework (Inclusive of fraud) at the operational level, Management level, Executive reporting, and the Board of Directors.

3.2. There are also specific internal controls in place at all the Group's operations (1st Line of Defence) that aim as primary enablers the duty to prevent fraud and corruption, and they include:

(a) whistle-blowing process (Group-wide fraud reporting facility);

(b) physical controls (securing of assets);

(c) authorisation controls (approval of expenditure);

(d) supervisory controls (supervising day-to-day issues);

(e) segregation of duties;

(f) monthly and annual financial statements;

(g) reconciliation of bank statements, monthly, and

(h) reconciliation of accounts, monthly.

3.3. The Group Human Resources Department participates in a pre-screening and continuous screening of staff members at all levels depending on the identified needs of the Group. There is also a process handled by the Group Human Resources Department to assist employees to achieve the relevant level of compliance to standards of operational excellence in their areas of operation, be it financial or educational training, e.g. FAIS training and other.

3.4 Secondary Enablers to Fraud and Corruption Prevention

3.4.1 Background and Introduction

(a) The Board of Directors of the Group has initiated a process of establishing a functional operational unit to deal with Corporate Governance, Risk Management, Fraud Prevention, Internal Audit, Compliance matters in the organisation. Heads of control functions take responsibility for all such activities (2nd and 3rd Line of Defence).

(b) Fraud Prevention Plan Activities to manage fraud and corruption within the Group.

3.4.2 The secondary enablers to fraud and corruption prevention within the Group form part of the Fraud prevention Plan activities and include:

3.4.2.1 Identification and assessment of vulnerable areas:

3.4.2.1.1 Risk Assessment

(a) The Group has identified potential fraud and corruption exposures within our current operating systems and procedures previously through interviews with specific employees, management, directors, and clients.

(b) The Risk Officer should conduct (as part of the Annual Risk Management Workshop, each year) a Fraud Risk Workshop from which potential exposures should be identified and recorded (through the Risk Registers). Operational Managers shall then design and implement further action to counter the exposures and, wherever possible, prevent or reduce the incidence of fraud and corruption in the future.

3.4.2.1.2 Due Diligence

(a) An appropriate level of due diligence must be performed on by the business on any business relationship with partners, agents, and intermediaries.

(b) Where the risk of bribery and corruption is perceived high, the level of due diligence must also increase.

(c) The due diligence must follow the risk-based approach based upon fraud risk assessments. These approaches should also take account of the financial value of the relationship. The simple matrix below is a guide to assist in the decision making.

Fraud/Bribery Risk	Example of due diligence requirements
Low	Financial Strength
	Period in business Basic reputation checks
Medium	All the above More formal reputational checks (registrations, internet checks, enquiries via local chamber of commerce)
High	All the above plus Establishing bona fides through external diligence agents or trusted external references

3.4.2.1.3 Employment screening practices

(a) The Group Human Resources Department participates in a pre-screening and continuous screening of staff members at all levels depending on the identified needs of the Group.

(b) Screening employees should also take place on promotions or transfers, particularly to high profile appointments such as Heads of Department or executive, Procurement, Claims Manager, key financial and IT positions.

3.4.2.1.4 Employee Training

(a) Employees should be trained on the identification and reporting of fraud, corruption, and bribery. They should also be trained to understanding the risk of engaging in activities of fraud, bribery and corruption.

3.4.2.1.5 Ownership of fraud and corruption risk management

(a) The Group's employees are responsible for the management of fraud and corruption risks, but the Board of Directors has the ultimate responsibility. The Board of Directors has delegated the responsibility of fraud risk management along with the flow of activities from strategic to operational level through the Fraud Risk Register and the ownership to management and specific identified staff members of the Group.

4. MANAGING FRAUD, BRIBERY & CORRUPTION RISK

4.1. Financial Controls

4.1.1 Financial controls should be such that they prevent making and receiving of bribes including proper authorisation process before any payment is made.

4.1.2 Proper selection of vendors, risk-based monitoring and third-party relationships and payments made.

4.2. Investigations

4.2.1 The Group is committed to investigating all internal/external fraud, corruption, theft, or associated irregularity suspected or discovered in an independent and objective manner.

4.2.2 All allegations of fraud must be properly investigated:

(a) Obtain a copy of the concern, complaint, or breach.

(b) Identify, secure, and obtain data in whatever form which includes changing of system access and locks if necessary.

(c) Obtain and analyse the documents.

(d) Conduct the initial validation and verification of the information received.

(e) Secure documents and relevant evidence related to the suspected fraud, including but not limited to, contents of the suspect's office or workstation, personal computer, and files.

(f) The Internal Audit function in conjunction with senior management will select and identify properly qualified and placed individuals to conduct the inquiry dependent on the scope of the investigation and the complexity, and nature of the matter reported.

4.3 Procurement and Contract management procedures

4.3.1 Procurement and contract management procedures must be in place to decrease the opportunity of fraud including the incorporation of anti-bribery and corruption provisions, termination, and audit rights in contracts with third parties.

4.4 Disclosure process

4.4.1 The following must be in place:

(a) Gift/Hospitality register containing all requests for approval and decisions made must be established and maintained.

(b) Appropriately senior and skilled employees must approve the granting or receiving of gifts/hospitality above a reasonable minimum level.

(c) declared gifts/hospitality must be reviewed at least annually.

4.5 External Reporting

4.5.1 Bribery and corruption cases must be promptly reported to local law enforcement (and regulatory bodies if appropriate), except where circumstances render this impractical or unsafe, and in which case they must be reported to the Head of Internal Audit or reported via the anonymous tip-off line.

4.6 Governance and Professional Ethics Statement

4.6.1 The Group is committed to the highest moral and ethical standards, openness, and accountability. All employees are expected to share the same commitment and lead by example in ensuring adherence to appropriate regulations, procedures, and practices. It is expected by the Group that individuals and organisations with whom it does business to act with honesty.

4.7 Ethical culture

4.7.1 The Group's staff and connected parties are required to always conduct themselves in an ethical and moral way that complies with the South African Constitution and the Group's core values. The Group's Human Resources Department has produced a Conflict-of-Interest Policy document that is applicable to all staff members including directors and is used to manage relationships with internal and external parties. The Group Human Resources Department has also issued a Code of Ethics/Code of Conduct applicable to all staff within the Group and which is provided to them at their employment date.

4.7.2 The Fraud Prevention Plan activities are to be supported by the following four pillars of fraud prevention:

(a) prevent and deter;

(b) detect;

(c) investigate; and

(d) resolve.

4.8 Prevention and Deterrence

4.8.1 The prevention and deterring of fraud and corruption is ongoing and a key enabler to achieving the Fraud Prevention Framework objectives.

4.8.2 These standard controls must be implemented as part of the prevention and deterrence of fraud and corruption within the Group:

(a) Code of Ethics;

(b) Conflict of Interest Policy for Internal and External parties;

(c) Communication as to fraud and corruption in the market;

(d) Compliance management;

(e) Enterprise-wide Risk Management;

(f) Training, Education and Awareness as to Fraud and Corruption; and

(g) Applying lessons learned to all operations.

4.9 Detection

4.9.1 Fraud and corruption is primarily detected through line management, internal reporting mechanisms, tip-offs, Whistle-Blowing and Internal and External Audit reviews.

4.10 Investigation

4.10.1 Depending on the type of fraud and/or corruption, there are different Investigation methodologies being used. The methods include, but are not limited to:

(a) Forensic Auditing techniques;

(b) Group Human Resources Policies and Procedures;

(c) Internal and External Audit procedures; and

(d) Facilities Security and Management Procedures.

4.11 Resolution

4.11.1 The investigations report from the fraud/corruption investigation will determine the appropriate resolution of the case, which may include inter alia: disciplinary action, civil/criminal proceeding. In addition, it is imperative after any investigation there are lessons learned, leading to control improvements and improved reporting processes.

5. ROLES AND RESPONSIBILITIES

5.1. Management

5.1.1 Management will be responsible for the development and implementation of the Fraud Risk Management Plan, including each manager and employee's responsibility for detecting fraud or related dishonest activities in their area of responsibility. Management and employees should be alert to the fact that unusual transactions or events could be symptomatic of an actual or attempted act of fraud, theft, corruption or associated internal/external irregularity.

5.1.2 Management will:

(a) Create a culture through words and actions making it clear that fraud is not tolerated. Any such behaviour will be dealt with swiftly and decisively and whistle-blowers will not suffer reprisal.

(b) Report to the board on what actions have been taken to manage the Fraud risk and report on the effectiveness of the fraud risk management plan. This includes the reporting of actual fraud as well.

(c) Establish and implement adequate internal controls, by designing and implementing Fraud control activities to prevent and detect fraud.

(d) Ensure that background checks are done on new and existing suppliers, business partners to identify any issues of financial health, ownership, reputation, and integrity that may represent an unacceptable risk to the group.

5.2 Staff

5.2.1 All levels of staff, including Management shall:

(a) Have a basic understanding of fraud and are aware of the red flags.

(b) Read and understand policies and procedures (e.g. fraud policy, code of ethics, disclosure procedures and all other relevant policies and procedures).

(c) Understand the roles within the internal control framework and how their work procedures have been designed to manage Fraud risks and how non-compliance may create an opportunity for fraud to occur or go undetected.

(d) Any employee who is unclear as to what may constitute fraud, theft or corruption may obtain guidance from Internal Audit or the Risk Officer.

(e) Co-operate with the investigation team.

(f) Report immediately if they believe or suspect there is evidence of irregular behaviour and that an incident of fraud may have occurred.

5.3 Group Internal Audit

5.3.1 Internal audit will:

(a) Be custodian of the Fraud policy.

(b) Be part of the Group's stakeholder management team with SAICB.

(c) Co-ordinate the fraud risk assessment process.

(d) Co-ordinate the compliance with the annual reviews of Fraud mitigation strategies in addition to the Fraud Risk Assessment by management.

(e) Review the adequacy of the risks identified by management and overriding of controls.

(f) Include the Fraud Risk Assessment in the annual audit plan.

(g) Act independently and have direct access to the audit committee.

(h) Manage or conduct investigations of suspected fraud cases.

(i) Keep a register and compare cases of all suspected fraud.

(j) Assist fraud investigators in collecting and preserving evidence.

6. REPORTING OF FRAUD

6.1. There are clear lines for reporting fraud and corruption by employees of the Group. The Group has developed a Fraud Hotline (Whistleblowing) that is available to all clients and staff of the Group that will also be utilised by all the associated companies. Fraud reporting must be followed by an investigation.

6.2. All employees have a duty to act in the best interests of their employer. Any suspected or identified act of fraud, theft, corruption or associated internal/external irregularity should therefore be reported to Internal Audit so that an independent and objective investigation can be conducted.

6.3. In the case that an employee reports fraud to his/her manager, the manager will inform Internal Audit.

6.4. The Group respects the right of the individual to retain anonymity when reporting fraud, theft or corruption or associated internal/external irregularities.

6.5. Employees (as defined in the Protected Disclosures Act, No. 26 of 2000 as amended) who report suspected fraud, theft, corruption or associated internal/external irregularities, have protection under the provisions of this act.

6.6. In essence, the Protected Disclosure Act protects an employee against dismissal or occupational prejudice where a disclosure has been made to the employer in good faith and in accordance with a procedure prescribed by the employer that meets the requirements of the Act.

6.7. The Group has implemented a safe and confidential process for employees to report suspected incidents of fraud. The details below can be used by employees to raise any concerns or suspicions of fraud and bribery:

6.7.1 **Report Fraud to Tip-Off Line 0800 014 577.**

7. EVALUATION AND MONITORING OF THE FRAUD PREVENTION

7.1. Evaluation of the effectiveness of the fraud prevention plan is vital to ensure that benefits of implementing are realised. The value is evaluated by measuring performance against pre-set goals, objectives and key performance indicators which are aligned to the overall goals and objectives of the Group.

7.2. Employees are, for the purpose of this policy: directors; permanent staff; fixed term contractors on our payroll; and temporary workers and consultants not on the payroll but engaged for a period of at least one month.

8. REVISION HISTORY

Version	Date	Author	Organisation	Revision
1.0	May 2020	Enterprise Risk Management	CRIH	Policy created
2.0	May 2022	Enterprise Risk Management	CRIH	Policy reviewed and updated
3.0	November 2023	PG Todd	CRIH	Policy reviewed and updated
4.0	November 2024	PG Todd	CRIH	Policy reviewed and updated

GOI3g.1 CRIH Fraud and Corruption Risk Management Plan-Nov 24

Final Audit Report 2025-01-21

Created:	2024-12-03
By:	Rene Kok (renek@conduitcapital.co.za)
Status:	Signed
Transaction ID:	CBJCHBCAABAAfv2yzB8lnvtCmiAtsU4PGg1OUmUitQao

"GOI3g.1 CRIH Fraud and Corruption Risk Management Plan-Nov 24" History

Document created by Rene Kok (renek@conduitcapital.co.za)
2024-12-03 - 1:04:10 PM GMT- IP address: 41.193.162.150

Document emailed to Thema Baloyi (thembab@gmail.com) for signature
2024-12-03 - 1:04:14 PM GMT

Document emailed to Lusani Mulaudzi (lusani.mulaudzi@gmail.com) for signature
2024-12-03 - 1:04:14 PM GMT

Email viewed by Lusani Mulaudzi (lusani.mulaudzi@gmail.com)
2024-12-03 - 4:10:13 PM GMT- IP address: 66.249.93.165

Document e-signed by Lusani Mulaudzi (lusani.mulaudzi@gmail.com)
Signature Date: 2024-12-03 - 4:11:51 PM GMT - Time Source: server- IP address: 197.245.101.139

Email viewed by Thema Baloyi (thembab@gmail.com)
2024-12-03 - 7:54:53 PM GMT- IP address: 104.28.46.78

Email viewed by Thema Baloyi (thembab@gmail.com)
2024-12-10 - 8:49:06 PM GMT- IP address: 104.28.46.79

Email viewed by Thema Baloyi (thembab@gmail.com)
2024-12-17 - 10:19:40 PM GMT- IP address: 172.225.142.145

Email viewed by Thema Baloyi (thembab@gmail.com)
2024-12-24 - 8:27:20 PM GMT- IP address: 172.225.142.153

Email viewed by Thema Baloyi (thembab@gmail.com)
2024-12-31 - 1:26:01 PM GMT- IP address: 104.28.46.78

Email viewed by Thema Baloyi (thembab@gmail.com)

2025-01-07 - 3:21:23 PM GMT- IP address: 172.225.142.154

Email viewed by Thema Baloyi (thembab@gmail.com)

2025-01-14 - 8:43:13 PM GMT- IP address: 104.28.46.78

Email viewed by Thema Baloyi (thembab@gmail.com)

2025-01-21 - 1:24:04 PM GMT- IP address: 196.192.169.198

Signer Thema Baloyi (thembab@gmail.com) entered name at signing as Themba Baloyi

2025-01-21 - 1:24:56 PM GMT- IP address: 196.192.169.198

Document e-signed by Themba Baloyi (thembab@gmail.com)

Signature Date: 2025-01-21 - 1:24:58 PM GMT - Time Source: server- IP address: 196.192.169.198

Agreement completed.

2025-01-21 - 1:24:58 PM GMT