

Alexander Forbes Group Holdings Limited

GROUP ECONOMIC CRIME AND FRAUD RISK
MANAGEMENT POLICY

Document Information

Policy Owner	Group Ethics Committee
Creation date	19 January 2009
Latest approval date	7 March 2013
Approval by	Alexander Forbes Group Holdings Limited Audit and Risk Committee
Latest review date	July 2020
Version	3.0

TABLE OF CONTENTS

Document Information2

1. Definitions.....4

2. Introduction.....5

3. Purpose5

4. Risk Appetite Statement.....5

5. Scope6

6. Economic Crime Risk Management Strategy6

7. Roles and Responsibilities7

8. Reporting.....13

9. Legislative and Best Practice frameworks13

10. Other relevant Policies and Documents.....14

11. Approval and Review of Policy.....15

Appendix A: Economic Crime Risk Management Strategy16

Appendix B: Examples of Actions Constituting Fraud, Theft, Corruption and Cybercrime19

Appendix C: Prudential Standard Requirements20

Appendix D: COSO Fraud Framework.....21

1. Definitions

Employees	Includes all permanent staff, temporary staff and consultants
Management	The line of business management structures
External Stakeholders	Clients, other service providers, contractors, strategic alliances, joint venture partners and any other party with a business relationship with the organisation
Corruption	Any conduct or behaviour when a person accepts, agrees or offers any gratification for him/herself or for another person where the purpose is to act dishonestly or illegally. Such behaviour also includes the misuse of material or information, abusing a position of authority or a breach of trust or violation of duty or as more fully defined in the Prevention and Combating of Corrupt Activities Act of 2004 or any other relevant legislation.
Fraud	Any unlawful act or omission by which a misrepresentation is made with the intention to defraud which causes actual prejudice or which is potentially prejudicial to another, whether or not there is personal benefit to the perpetrator. Internal fraud is perpetrated by employees, while external fraud could be perpetrated by stakeholders (as indicated above)
Theft	Defined, among other things, as an appropriation of property belonging to another with the intention of permanently depriving the owner of the use and possession of that property
Irregular activity	An action considered irregular is defined, among other things, as an activity that is contrary to company policies, regulations, procedures, laws, or activities that are unethical in nature or not conforming to generally accepted business practices
Economic Crime	Refers to illegal acts committed by an individual or a group of individuals to obtain a financial or professional advantage, and which include the following activities: <ul style="list-style-type: none"> ○ Asset Misappropriation ○ Fraud committed by the consumer ○ Procurement fraud ○ Bribery & corruption ○ Business conduct / misconduct ○ Cybercrime ○ Human Resources fraud ○ Accounting fraud ○ Money laundering ○ Intellectual Property theft ○ Competition / Anti - Trust Law infringement ○ Insider trading ○ Tax fraud ○ Extortion ○ Forgery ○ Collusion or conspiracy ○ Any other deception, false representation, concealment of material facts or unethical behaviour

2. Introduction

The Board of Directors of Alexander Forbes and its subsidiaries has committed Alexander Forbes to a process of preventing crime, which is aligned to the King IV Report and complies with other relevant legislation, regulation and guidelines. The prevention of economic crime is recognised as being an integral part of good corporate governance. The Economic Crime and Fraud Risk Management policy will be applicable across all Alexander Forbes operations, including business units across the organisation, as well as to strategic alliance and joint venture partners.

The effective deterrence, prevention, detection and response to economic crime and fraud (*hereafter collectively referred to as economic crime*) is imperative for Alexander Forbes, where its reputation is one of its greatest assets. The effective implementation of this policy will complement the realisation of Alexander Forbes' strategy and will protect the direct interests of stakeholders, shareholders, staff and the communities in which it operates. Sound management of Alexander Forbes' exposure to economic crime will enable it to anticipate and respond to changes in the business practices and processes.

An enterprise-wide approach to the deterrence, prevention, detection and response to economic crime will be adopted by Alexander Forbes. Identified exposures to economic crime will be included in the structured and systematic process of risk management.

The Social and Ethics Committee is required to confirm to the Board of Directors annually that the economic crime deterrence, prevention, detection and response processes are operating effectively. Every director, manager and employee have a key role to fulfil in implementing this policy.

3. Purpose

- 3.1 As part of the overall corporate governance framework and in furtherance of the sound operation of Alexander Forbes Group Holdings Limited ("the Group"), the Board of Directors is responsible for overseeing that the Group has in place effective systems and functions to address the key risks it faces and to satisfy key legal and regulatory obligations. Managing economic crime risk should be seen in the context of the management of this wider range of risks.
- 3.2 The purpose of this policy is to establish the principles and standards for managing economic crime risks and in doing so, limit the exposure of the organisation to fraud, theft and corruption.
- 3.3 The principles outlined in this policy along with the implementation of initiatives per the Economic Crime and Fraud Risk Management Strategy (section 4) seek to embed fraud risk management practices into the day-to-day management activities in efforts to limit the exposure of the organisation to economic crime.

4. Risk Appetite Statement

- 4.1 Alexander Forbes views wilful non-compliance with legislation, any criminal activity and transgressions of internal rules, policies and procedures as well as its values in an extremely serious light and as such has a zero tolerance to such actions and matters.
- 4.2 A zero-tolerance approach implies that Alexander Forbes will encourage, allow and support the investigation of any employee or stakeholder, regardless of status or stature, implicated in any form of irregular activity in or against Alexander Forbes. No employee, irrespective of seniority or association, will be exonerated from this principle. The investigations will be conducted in a transparent and fair manner, taking into account the constitutional rights to privacy and a fair hearing.

5. Scope

- 5.1 The content of this Policy must be read in conjunction with all relevant values expressions, charters, policies, procedures, frameworks and similar documents of Alexander Forbes.
- 5.2 This policy applies consistently to all employees and stakeholders in the Alexander Forbes Group (which include all its legal entities and business units) (“the Group”) and must be read with any other like policy that may be applicable to an employee in a specific business unit, or to an employee arising from his or her relationship or affiliation with any professional or other body.
- 5.3 This policy applies to any economic crime, fraudulent, dishonest or corrupt activity, or suspected fraudulent, economic crime, dishonest or corrupt activity, involving employees and any other Alexander Forbes Group Stakeholder.
- 5.4 Business areas situated in other jurisdictions will be subject to the principles stated herein, insofar as these principles do not contradict requirements of that foreign jurisdiction. The interpretation of applicable foreign legislation and common law shall be obtained from a reputable source resident within the foreign jurisdiction concerned.

6. Economic Crime Risk Management Strategy

- 6.1 The Group aims to limit its exposure to economic crime and fraud by implementing an appropriate economic crime risk management strategy that involves prevention, detection and response activities. The diagram below sets out the various initiatives which form part of the holistic fraud risk management strategy:



- 6.2 The specific preventative, detective and responsive initiatives / mechanisms that Alexander Forbes will implement, roll out and manage will be detailed in the Economic Crime Risk Management Programme in support of this policy. Refer to **Appendix A** for the detailed Economic Crime Risk Strategy initiatives.

Appendix B sets out the examples of Fraud, Theft and Corruption that this strategy would respond/address through the various initiatives.

6.3 As a minimum, the preventative, detective and responsive initiatives documented within the policy should be included within the implementation programme. Where necessary, additional initiatives or activities may be introduced within this programme as the economic crime approach matures.

6.4 The preventative, detective and response initiatives and mechanisms will assist Alexander Forbes to:

- Assist the organisation to identify, prioritise and address the major economic crime risks of the organisation;
- Define roles and responsibilities in relation to the execution and management of the Economic Crime Risk Management Programme;
- Assist in evaluating and enhancing the Economic Crime Risk Management Programme regularly (preferably on an annual basis); and
- Outline the importance of internal and external compliance or integrity or economic crime risk management communication.

7. Roles and Responsibilities

The table below outlines the roles and responsibilities of the Group stakeholders responsible for governance of this Policy:

Structure	Duties and Responsibilities
Supervision of these activities	
Group Social, Ethics and Transformation Committee	<p>To set the appropriate tone for the organisation, the board is responsible for ensuring that management designs an effective Economic Crime Risk Management Programme by mandating the SET Committee to:</p> <ul style="list-style-type: none"> ● Periodically reviewing management’s Economic Crime and Fraud Risk Management Policy, as well as other applicable policies and procedures of the organisation designed to help mitigate economic crime; ● Monitoring management’s reports on economic crime risks, policies, and control activities; ● Assessing the risk of economic crime by management, including the risk of management’s override of controls, and ensuring that controls are designed and functioning to deter prevent, and detect economic crime by management; ● Being fully informed about instances of economic crime that occur within the organisation, in particular, instances involving senior-level employees or employees about whom significant internal control issues are uncovered; ● Monitor management’s application of the disciplinary policy during disciplinary and corrective action, to ensure that the disciplinary policy in so far as it relates to economic crime, is uniformly applied throughout the organisation;

Structure	Duties and Responsibilities
	<ul style="list-style-type: none"> Ensuring that management has assigned sufficient resources to execute on the activities necessary to operationalise this policy and the supporting implementation plan; and Retaining outside advisors and counsel, as necessary.
Group Audit & Risk Committee	<ul style="list-style-type: none"> Being fully informed about instances of economic crime that occur within the organisation, in particular, instances involving senior-level employees or employees about whom significant internal control issues are uncovered and have resulted in financial loss; and If fraud or any actions that may affect the company's financial stability, income or reputation is committed, the audit committee must report the findings to the company's board of directors in order to rectify within the appropriate period as deemed by the committee, without delay.
Operational Implementation	
Ethics Management Committee	<ul style="list-style-type: none"> Review all ethics related reports received, including whistle blower reports and determine the most appropriate investigation, consequence management and remedial actions; and The Committee has the explicit mandate to direct line management to take appropriate actions or remedial steps in respect of whistle blower reports.
Management	<p>Management has overall responsibility for the implementation of this policy and the implementation programme:</p> <ul style="list-style-type: none"> Implement and maintain strategies and operational functionalities, in collaboration with the Group Forensics Services (GFS) to manage the risk of economic crime activities (this would extend to 3rd parties/joint ventures); Reporting to the board about economic crime risk matters; Identifying and assigning personnel responsible for anti-fraud control activities and maintaining records that verify that those processes and controls have been properly executed; Providing defined, proactive processes and control activities to prevent, detect and react to economic crime; Implementing internal controls designed to prevent and/or detect fraud within each business unit;

Structure	Duties and Responsibilities
	<ul style="list-style-type: none"> • Developing training and awareness activities to promote understanding and compliance with all economic crime related policies; • Maintaining an open-door policy and other mechanisms to report economic crime; • Monitoring the successful completion of disciplinary and corrective action, when assigned; • Actively and timeously consider the recommendations made by GFS or other parties as it relates to the risk of unlawful and unethical conduct. Management accepts that it is responsible and ultimately accountable for responding to risks by ensuring that weaknesses identified in the control environment are adequately and effectively addressed to prevent past events from recurring and the prevention and detection of future events; and • Prevent concentration of risk by continuously documenting control failures in the agreed format and continuously review and assess control failure/weakness.
Employees	<p>Strong controls against economic crime are the responsibility of everyone in the organisation. All levels of personnel within Alexander Forbes will:</p> <ul style="list-style-type: none"> • Have a basic understanding of economic crime, be aware of red flags, be familiar with the types of economic crime that might occur within their areas of responsibility, and be alert to any indications of economic crime; • Understand their roles within the internal control framework. Personnel must understand how their job procedures are designed to manage economic crime risks and when non-compliance may create an opportunity for economic crime to occur or go undetected; • Read, understand and affirm Alexander Forbes’s related policies and procedures designed to mitigate economic crime; • As required, participate in the process of creating a strong control environment and designing and implementing economic crime control activities, as well as participate in monitoring activities; • Report concerns, suspicions or incidences of fraud as set out in the whistle-blowers policy; and • Cooperate with investigations.

Structure	Duties and Responsibilities
Human Resources	<p>The human resources department assists management and employees by executing key anti-fraud control activities through on-boarding, training, counselling, and issue resolution activities and processes, including:</p> <ul style="list-style-type: none"> • Screening of employee candidates and periodic updates to employee background investigations; • Facilitating new employee orientation and other employee training activities, which includes the annual review and affirmation of key corporate policies; • Conducting, analysing and reporting on the results of employee satisfaction and fraud related matters; • Escalating issues involving potential economic crime reported by management and employees; • Participating in management’s economic crime risk assessment activities; • Reviewing resignation letters and conducting exit interviews in order to identify and escalate any potential concerns or complaints related to economic crime; • Supporting internal investigation activities, as needed; and • Monitoring the disposition of disciplinary or correction action, when administered and ensure that the disciplinary policy is uniformly applied across the organisation.
Group Legal	<p>The legal department advises management on the following:</p> <ul style="list-style-type: none"> ■ Participating in the creation of key policies and procedures of the organisation; ■ Guiding the escalation, assessment, investigation and closure of allegations involving economic crime; ■ Participating in the flow of information about investigations to senior management and relevant committees, as well as regulators and law enforcement, as appropriate; ■ Assisting in the recovery of lost assets due to fraud and misconduct; ■ Providing communication regarding litigation and other asset recovery efforts on a periodic basis to the audit and risk committee; ■ Participating in management’s economic crime risk assessment, as well as awareness and training activities; and ■ Implementing, tracking and communicating new legislative and regulatory requirements.

Structure	Duties and Responsibilities
<p>Group Forensic Services (GFS)</p>	<p>Collaborating with management to develop, implement and maintain strategic and operational anti-economic crime programs and processes, that include processes and initiatives to continuously prevent, detect and respond to economic crime, by enabling and using continuous data mining and analytical exercises on all appropriate data and processes, where required or deemed necessary;</p> <ul style="list-style-type: none"> ■ Assisting management with the implementation of improved processes and procedures to pro-actively identify potential future incidents of unlawful and unethical conduct based on knowledge gained from responding to incidents; ■ Investigating identified incidents in a timeous manner, with the aim of establishing material facts, collating relevant evidence and making appropriate recommendations for corrective action and/or prosecution. All investigation activities should adhere to an agreed standard; ■ Ensure in conjunction with HR, that appropriate disciplinary processes and/or prosecution procedures are applied in a consistent manner in line with the zero tolerance risk appetite; ■ Implementing appropriate record keeping procedures in respect of suspicious incidents and investigations in the form of a case management system and a risk register as to enable the reporting of the progress, outcome and conclusion of investigations and to procure data for proactive initiatives such as a maintaining a RedFlag System, ensuring that data exists for supporting enhancements to control environments etc; ■ Informing all stakeholders timeously of significant investigations initiated and of significant control breakdowns identified, where appropriate; ■ Ensuring that, where necessary, all investigated cases are reported to relevant authorities and where applicable, appropriate action for restitution is instituted; ■ Implementing and managing processes and procedures in collaboration with business to maximise the recovery of any losses incurred; ■ Ensure in conjunction with management and industrial relations/human resources functions that an effective, reasonable, transparent and consistent disciplinary approach exists and is utilised as to deal with employees that have transgressed; ■ Assisting business and the risk function when conducting economic crime risk assessments; ■ Ensuring that adequate staffing and infrastructure is in place at GFS to fulfil the responsibilities as outlined in this Policy; ■ Ensuring implementation, usage and maintenance of independent reporting structures such as anonymous hotlines and online reporting facilities in collaboration with business; ■ Applying oversight processes to the activities of other forensic units (where applicable) to ensure compliance with this Policy;

Structure	Duties and Responsibilities
	<ul style="list-style-type: none"> ■ Ensuring compliance with this Policy and fulfilling reporting requirements to various stakeholders; and ■ Ensuring adequate engagement and participation with industry bodies related to economic crime risk mitigation- e.g. FSCA, ASISA, ACFE, PA, SAICB etc.
<p>Group Internal Audit (See note 1 below)</p>	<p>The internal audit department provides independent, objective assurance regarding the design and operating effectiveness of management’s anti-fraud controls, including:</p> <ul style="list-style-type: none"> ■ Evaluating the potential for the occurrence of fraud and how Alexander Forbes manages economic crime through walk-throughs and review of Alexander Forbes Fraud Risk Management Programme; ■ Assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of controls commensurate with the extent of the potential exposure/risk in various segments of the Alexander Forbes operations; ■ Ensuring that management has reviewed its risk exposure and identified the possibility of economic crime as a business risk through an economic crime / fraud risk assessment; ■ Incorporating information about fraud obtained through the fraud risk assessment process, reporting mechanisms and investigations with the annual internal audit plan; ■ Ensuring that management has actively and timeously considered the recommendations made by GFS and ensured that that weaknesses in the control environment identified by GFS and Group Internal Audit are adequately and effectively addressed to prevent past events from recurring and the prevention and detection of future events; ■ Ensuring that management revisit internal controls at regular intervals to ensure they remain responsive to current and emerging economic crime risk; and ■ Delivering information to the audit committee about the adequacy of management’s arrangements for mitigating economic crime and ensuring that Alexander Forbes promotes an anti-fraud culture.

Note (1): The Group Forensics Services function currently reports into the Chief Audit Executive. As such this creates a conflict in terms of the work that Group Internal Audit can perform in terms of independent assurance. Independent assurance around the adequacy and effectiveness of the organisation’s fraud risk programme/approach would need to be undertaken by an external party until this has been fully handed over to business.

8. Reporting

This section outlines the reporting to regulatory authorities as well as engagement with applicable industry bodies to contribute towards the prevent, detection and remediation of fraud across the industry. It also outlines the internal reporting mechanisms.

8.1 SAPS:

The purpose of the Group Investigation Policy is to establish a framework for investigating, reporting and responding in the event that suspected economic crime, fraud, theft or corruption is detected. The Group Investigation Policy states that in terms of the requirements of the Prevention and Combating of Corrupt Activities Act 12 of 2004, any potential crime to the value of R100 000 or more must be reported to the South African Police Services. Group Forensic Services (GFS) will be responsible for reporting crime in line with the approved procedures.

Refer to the Group Investigation Policy for further information on reporting.

8.2 South African Revenue Service (SARS), Financial Sector Conduct Authority (FSCA), Prudential Authority (PA) etc.:

GFS will report incidents of economic crime, fraud, corruption and theft to the relevant authorities, including but not limited to SARS, Financial Sector Conduct Authority (FSCA), etc. where applicable and in line with the required legislation. This will be done in consultation with the applicable compliance officer. All incidences reported to the relevant authorities will be forwarded to the Ethics Committee. The Ethics Committee will compare all matters reported to the fraud tracker to ensure that all matters are reported.

The Group Investigation Policy will provide further information on reporting.

8.3 Insurance Crime Bureau (ICB):

Alexander Forbes is a member of the Insurance Crime Bureau which is dedicated to fighting organised insurance crimes and fraud. The Insurance Crime Bureau is supported by law enforcement and industry partners that provide its members with access to fraud prevention and detection initiatives, insurance fraud investigations, training and public awareness. Being a member of this organisation is an example of how Alexander Forbes contributes to industry wide initiatives to deter, prevent, detect, report and remedy insurance fraud.

8.4 Whistleblowing:

Every Alexander Forbes employee must report any suspected or actual unlawful or irregular activity, whether that activity has been or is in the process of being committed or contemplated by an employee (which includes directors and management), clients and service providers, outside parties and/or any other legal entity. The reporting of such instances is guided by the Whistleblowers policy and procedure.

9. Legislative and Best Practice frameworks

9.1 This framework has been drafted in consideration of the requirements under the Prudential Standards supporting the Insurance Act No. 18 of 2017 as set out in the following documents (**Refer to Appendix C**):

- Prudential Standard GOI 3; and
- Prudential Standard GOG.

9.2 Various regulations are relevant to the anti-corruption and anti-fraud strategy and serve to supplement each other in the combating of corruption and fraud. Some of the most important Acts are:

- The Constitution of the Republic of South Africa, 1996.
- The Companies Act of South Africa No. 71 of 2008 (and supporting regulations).
- The Prevention and Combating of Corrupt Activities Act, No 12 of 2004.
- The Protected Disclosures Act, No 26 of 2000
- The Promotion of Administrative Justice Act, No 3 of 2000
- The Prevention of Organised Crime Act, No 121 of 1998

9.3 Furthermore, the Framework is based on the principles embodied in the Committee of Sponsoring Organizations of the Treadway Commission (COSO), Fraud Framework 2016. **Refer to Appendix D.**

9.4 King IV Report on Corporate Governance for South Africa 2016 (King IV).

10. Other relevant Policies and Documents

10.1 This policy should be read in conjunction with the following policies, framework, programmes:

#	Policy/Guideline	Applicability
1.	Corporate Governance Framework	Governed by
2.	Enterprise Risk Management Strategy, Framework and Policies (especially the Group Operational Risk Management Policy)	Governed by
3.	Group Internal Control Policy	Governed by
4.	Code of Ethics Policy	Alignment and contribution
5.	Disciplinary Policy	Alignment and contribution
6.	Conflict of Interest Policy	Alignment and contribution
7.	Procurement Policy	Alignment and contribution
8.	Gift and Entertainment Policy	Alignment and contribution
9.	Group Investigation Policy (in development)	Supports implementation of this policy
10.	Whistleblowing Policy	Supports implementation of this policy
11.	Anti-Bribery and Anti-Corruption Policy	Alignment and contribution
12.	Anti-Money Laundering Policy	Alignment and contribution
13.	Fraud Awareness Programme	Supports implementation of this policy
14.	Economic Crime Risk Management Programme	Supports implementation of this policy

11. Approval and Review of Policy

This policy will be periodically assessed to determine whether the purpose, authority, and responsibility, as defined in this policy, continue to be adequate to enable the Group to accomplish its objectives. Ad hoc reviews may be prompted in the event of an incident that may materially affect Alexander Forbes financial stability or credibility.

The policy must be updated at least once a year, or more frequently as circumstances may necessitate. It must be approved by the Social, Ethics and Transformation Committee.

Appendix A: Economic Crime Risk Management Strategy

Alexander Forbes Economic Crime Risk Management strategy focuses on prevention, detection, response that collectively result in fraud deterrence.

The detailed initiatives underpinning the fraud risk management strategy include:

1. Board Oversight / Management Responsibility

The starting point for any Fraud Risk Strategy is the tone at the top. Most initiatives fail because they lack the proper executive sponsorship or are not well communicated across the organisation.

The same is true with crime. People commit crime. As a result, establishing the proper tone and communicating Alexander Forbes' position regarding crime is a critical step in making the Fraud Risk Management Strategy effective. Additionally, it is not enough to communicate the organisation's crime concern once or twice, it must be reiterated, discussed, and debated continuously so that it becomes part of the Alexander Forbes culture. Any remedial action taken by management should also be communicated so that it sets a zero-tolerance tone from the top.

2. Prevent

2.1 Code of Conduct

A Code of Ethics are principles in which management of Alexander Forbes believes and requires all employees to subscribe to. A Code of Ethics sets the guidelines that lead employees towards acting in the fashion that is consistent with the organisation's values.

Each employee is expected to sign an acknowledgement that they understand that failure to abide by the provisions outlined in the Code of Ethics may result in disciplinary action and criminal or civil proceedings against them. Linked to this, employees should also acknowledge that they have a role to play in the identification, prevention and management of economic crime.

2.2 Policies, procedures, processes and controls

Fraud/Economic crime related policies will guide employees through complex issues, provide a channel for employees or third parties to report fraud and economic crime, establish procedures to govern the escalation of fraud/economic crime allegations, and provide support/protection for whistleblowers.

The fraud/economic crime related policies would include Alexander Forbes' policy stance to economic crime and steps for the reporting, basic investigation and resolution of allegations and incidents of economic crime.

2.3 Education and Advice

Fraud & Economic Crime Awareness training focuses on educating employees on the Code of Ethics, understanding protocols for reporting suspicious activity and communicating the disciplinary actions that may be taken in the event of economic crime occurring. Continued training, education and advice is essential to keep new and existing employees abreast of the control and ethical environment. A Fraud Awareness Programme will be implemented that will detail all awareness initiatives linked to economic crime.

2.4 Legislative Compliance

The Fraud Risk Management Strategy should include mechanisms to monitor compliance with all applicable laws, rules, and regulations, and keep up to date with changes in such laws, rules and regulations. A specific regulatory universe linked to all legislation and good governance practices should be developed and maintained.

3. DETECT

3.1 Speaking up & Confidential reporting

Alexander Forbes will continue to ensure the existence of the anonymous Whistleblowers Line which all stakeholders can use to report suspected fraud/economic crime or unethical behaviour.

Alexander Forbes has put in place such a mechanism in terms of which employees and outsiders are encouraged to pass on any information or reasonable suspicions on economic crime that they may believe to have occurred. Mechanisms have been put in place to ensure that such information or suspicions are channelled through Alexander Forbes Governance Office and to the relevant executives who will deal with them appropriately.

Should the information received through the Whistle-blowers Line be useful and result in economic crime being uncovered, appropriate action/steps shall be taken against the perpetrator.

As it is unavoidable that information on non-economic crime related matters is also received, provision is made for communicating such information to the relevant business unit. Such information is not automatically ignored as it may result in the whistleblower losing faith in the system.

3.2 Third Party Diligence

Conducting active screening of third parties would ensure that the organisation limits its exposure and reputational damage from potential fraudsters.

The effectiveness of internal controls is diminished through related party transactions, conflicts of interest or collusion. This may take place between internal employees or between employees and external parties. Conflicts of interest will therefore be considered and investigated for links between internal and external parties and between business units.

3.3 Monitoring Reviews & Auditing

In order to identify controls to help prevent economic crime it is necessary to understand which processes have potential weaknesses and may be susceptible to economic crime. This insight will be gained through testing those processes and systems for the vulnerability of economic crime and collusion occurring, by conducting simulated, authorised, irregular criminal attempts.

Economic crime / fraud risk assessments, surprise audits and vulnerability reviews should be carried out in order to provide a proactive process to uncover economic crime and to provide a deterrent to potential fraudsters.

Internal controls are to be revisited at regular intervals to ensure they remain responsive to current and emerging economic crime risk.

3.4 Data Analytics

Data analytics is the 'mirror' that will be used to evaluate the effectiveness and efficiency of the enhanced Fraud Risk Management strategy. This is an on-going cycle of continuous root cause evaluation to better align the Fraud Risk Management Strategy to the business risks facing the organisation.

GFS should utilise appropriate resources (e.g. specialised software) in order to proactively find the "red flags" of unexpected conflicts of interests, duplicate payments and other irregularities that are normally hidden in large data sources.

4. RESPOND

4.1 Incident and Case Management

A case management system is implemented and utilised to track, manage and monitor internal investigations. The case management system serves as a central repository for retaining evidence and reporting back to management in relation to the investigation outcomes.

4.2 Investigation

All allegations received through the Whistleblowing mechanism and from management via the internal fraud email box are investigated to establish if the allegations were founded or to establish whether there was any form of non-compliance with legislation and / or policies and procedures.

4.3 Corrective Action

Subsequent to investigations being performed and sufficient evidence being located and documented, it will be necessary for Alexander Forbes to institute the necessary corrective action which will include: disciplinary, civil and / or corrective action.

4.4 Remediation

The key root causes of the internal control breakdowns identified by Internal Audit, through internal audits, investigations and proactive data analytics, will provide guidance on key focus areas to conduct such audits and further enhance the Economic Crime Prevention Strategy.

Appendix B: Examples of Actions Constituting Fraud, Theft, Corruption and Cybercrime

- Forgery or alteration of a bank draft or any other financial document or account belonging to a shareholder/stakeholder
- Misappropriation of funds, securities, supplies or any other assets belonging to Alexander Forbes, another employee, a customer, supplier or any third party
- Impropriety in the handling or reporting of money or financial transactions
- Profiting as a result of insider knowledge of securities activities
- Disclosing to other persons the securities activities engaged in or contemplated by Alexander Forbes
- Accepting or seeking (gifts, bribes/kickbacks) anything of (material) value from vendors or persons providing services/material to Alexander Forbes / payment or receipt of bribes (example would be kickback for a favourable outcome relating to a due diligence check on a 3rd party/asset manager).
- Destruction or removal of records, furniture, fixtures or equipment
- Disclosing confidential and proprietary information to outside parties
- Collusion
- Falsifying or manipulating financial records to cover up an irregular or illegal act, making detection of misappropriation of funds or assets difficult
- Intentional provision of false and/or incomplete information, concealment or misrepresentation of events or data (e.g. accounting records)
- Claims submitted for services or goods that were not actually provided to Alexander Forbes
- Deception and extortion
- Intentional non-compliance with any statutory legal requirement
- Deliberately omitting or refusing to report or act upon reports of any irregular or dishonest conduct
- Any similar or related irregularity
- Forgery or alteration of any document
- Insurance related fraud: for example, customers faking an insurance event, inflating losses, double claiming, etc.
- Investment related fraud: for example, manipulation of investment valuations, misclassification of investment gains and losses, etc.
- Cybercrime: for example, phishing, malware, cyberattacks to disrupt / steal money / steal IP.

Note: The above list is not comprehensive and serves as examples only.

Appendix C: Prudential Standard Requirements

This section indicates where the requirements under the Prudential Standards as per the Insurance Act have been addressed by the Group Fraud Risk Management Policy. To note that there are supporting policies and procedures that further address these requirements.

Prudential Standard Requirement				
Std	Section	Sub-Section	Regulatory Requirements	Policy Section
GOI 3.3	Attachment 1: Policies for Managing Financial Risks	G1	Outline appropriate strategies, procedures, and controls to deter, prevent, detect, report and remedy insurance fraud	Section 6 and Appendix A
		G2	Outline appropriate strategies for managing fraud risk and the risk to the insurer's financial soundness or sustainability caused by fraud	Economic Crime Risk Management Strategy supported by the Economic Crime Risk Management Implementation Programme. Section 6, 7 and Section 11.
		G3	Take into consideration how the effectiveness of fraud risk management may be enhanced by contributing to industry-wide initiatives to deter, prevent, detect, report, and remedy insurance fraud	Section 8.
		G4	Provide for the prompt reporting of insurance fraud to relevant regulatory authorities	Section 8.

Appendix D: COSO Fraud Framework

In order to comply with the Fraud Risk Management Principles per the COSO 2016 Fraud Framework, Alexander Forbes has developed an Economic Crime Risk Management Programme (“ECRMP”) where specific initiatives have been designed to address the leading practice requirements and at the same time operationalise the fraud risk strategies outlined in this policy. Roles and responsibilities for the ECRMP are detailed below. The fraud risk management principles as per the COSO Framework have been addressed as follows:

1. Control environment: *“The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk”.*
 - Alexander Forbes has developed an ECRMP. The ECRMP will be rolled out and executed by Group Forensics and the business. The ECRMP has a multi-dimensional focus that is aligned to preventative, detective and responsive initiatives as detailed in the strategy section (Section 6 and Appendix A).
2. Risk Assessment: *“The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks”.*
 - The ECRMP requires that a fraud risk assessment should be performed annually. The purpose of the annual fraud risk assessment is to identify fraud risks, assess their likelihood and impact, evaluate existing controls used to mitigate the risk and implement action plans to manage fraud risks.
3. Control Activities: *“The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner”.*
 - The ECRMP includes preventative and detective initiatives to roll out the Alexander Forbes fraud risk management strategy.
 - The ECRMP will consider and implement initiatives that monitor fraud losses which affect the financial soundness or sustainability caused by economic crime.
4. Information and communication: *“The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner”.*
 - The ECRMP includes the roll out and implementation of a Fraud Awareness Programme which details the specific fraud awareness activities to communicate and make key stakeholders aware of economic crime.
 - The ECRMP includes reactive initiatives that deal with the investigation of allegations and ensuring that corrective action ensues in relation to disciplinary, criminal and civil action including addressing weaknesses in controls.

5. Monitoring Activities: *“The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors”.*
 - The ECRMP will be reviewed on an annual basis by the Ethics Committee to ensure that the five COSO principles of fraud risk management are present and functioning.