Britam Policy Template
FOR INTERNAL USE

BRITAM GROUP

FRAUD RISK MANAGEMENT ("FRM") POLICY

Policy Owner: Group Managing Director

Last Committee Review: 5 June 2017

Date Last Update: 5 June 2017

Britam
With you every step of the way

Table of Contents

1. Document Change History

Policy version control			
Amendment Number	**Date**	**Approved by**	**Description of change**
0.0	14 September 2016	Stephen Omuga (Forensics Manager)	Origination of Policy
1.0	December 2016	Steve Magati (Group Head of Internal Audit)	Review
1.1	5 June 2017	Britam Holdings Board Audit Committee	Recommended for Board approval
2.0	6 June 2017	Britam Holdings Board	Board approval

Note: Number changes should reflect material changes/ reviews by a committee or policy owner. Point changes reflect minor changes.

2. Purpose

This Policy outlines the Britam approach to managing fraud. It:

- Defines what fraud means for Britam
- Sets out elements of the Fraud Risk Management Framework
- Articulates the roles and responsibilities of all access persons in proactively combating fraud, through prevention and detection controls
- Outlines required elements of an investigation response
- Defines the reporting requirements

3. Scope of the Policy

This policy applies to all types of fraud that may be experienced by Britam, regardless of origin.

This policy applies to all officers and employees of the Britam Group or any of its subsidiaries, financial agents and directors (collectively "access persons"). Management should ensure that all access persons are required to make themselves aware of this policy.

4. Definitions or abbreviation of words used in the policy

Fraud	Fraud is deceptive behavior intended to result in financial or personal gain or cause a loss to others. An act of fraud therefore occurs where a person: – dishonestly makes a false representation; – dishonestly fails to disclose information; or – dishonestly abuses a position of trust. In each case, there must be intent to make a gain or cause loss to another or expose another to a risk of loss.
False Representation	A representation is false if it is: • untrue and willfully made to deceive another to his damage; • untrue in fact, but recklessly made when the maker has no knowledge as to its truth or falsity; or • a promise made with no intention to carry it out.
Failure to disclose information	• A person wrongfully fails to disclose information to another person if s/he has a legal duty to disclose it; or the information is of a kind, which s/he is trusted to disclose, and it is reasonable to expect her/him to disclose it.
Abuse of position	• A person abuses a position of trust, when they have been given a position in which they are expected to safeguard another's financial interests and they abuse that position without the other's knowledge.
Theft	• A person is guilty of theft if s/he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it.

Fraud risk	• The vulnerability that an organization faces from individuals capable of combining all three elements in the fraud triangle, namely:
	  • Pressure – this is what motivates the act of fraud in the first place. The individual could for instance have a financial problem that he is unable to solve through legitimate means;
	  • Opportunity - Defines the method by which the crime can be committed. The person must see some way in which he can use (or abuse) his position of trust to solve his financial problem with low perceived risk of getting caught.
	  • Rationalization – The person must justify the fraud to himself or herself in a way that makes it an acceptable or justifiable act e.g. “I was only borrowing the money”, “I was entitled to the money”, “I had to steal to provide for my family” etc.

Access persons	Access persons refer to people who have direct or indirect access to sensitive company information. For purposes of this policy all officers and employees of the Britam Group or any of its subsidiaries (employed on a permanent, temporary or contract basis), financial advisors and directors are collectively referred to as access persons.

5. Policy Statements

5.1. Introduction

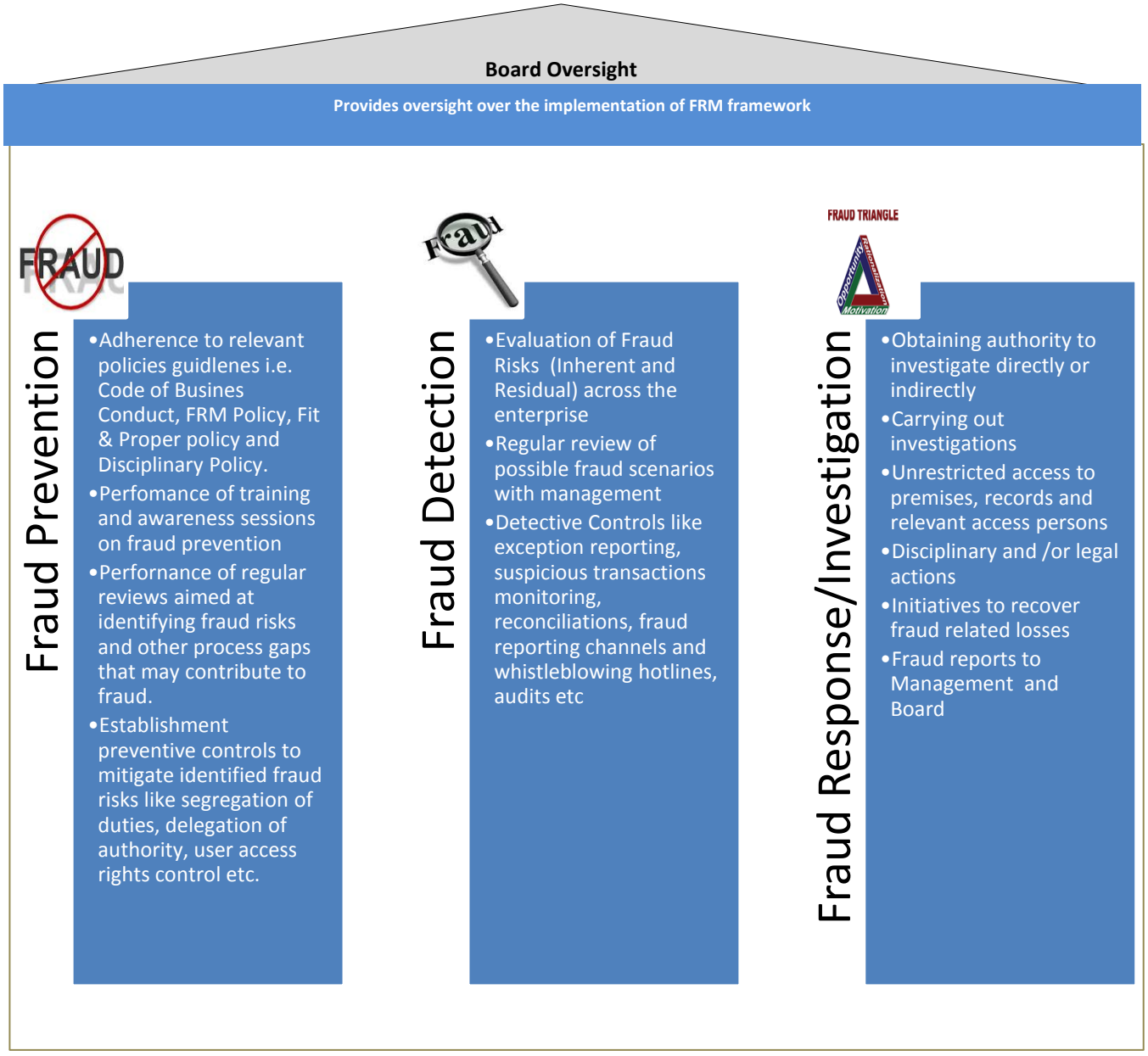
Britam is a leading diversified financial services group, listed on the Nairobi Securities Exchange and is committed to conducting its business according to the highest standards of honesty and fairness. This commitment to observing the highest ethical standards is designed not only to ensure compliance with applicable laws and regulations but also to earning and keeping the continued trust of our clients, shareholders, personnel and business partners.

Britam is committed to fraud control with an emphasis on proactive prevention and detection measures in an effort to reduce opportunities which could lead to fraud. The Company’s approach to fraud control centers on maintaining a legal and ethical environment which encourages all stakeholders to protect the Company’s assets and escalate any suspicion of fraud.

This policy is intended to establish certain minimum Company-wide requirements and guiding principles. Britam has a **zero tolerance to fraud**. When a fraud is detected, suspected or alleged, Britam will fully investigate the matter, and implement measures to recover and minimize any loss to the Company. Loss may be financial, reputational or regulatory. Britam also considers fraudulent, all intentional wrongdoings intended at causing a loss to Britam but detected before the occurrence of such loss. Internal controls will be reviewed in the light of materialized frauds to reinforce mitigation measures.

5.2. Fraud Risk Management Framework

The Britam FRM Framework is composed of 3 pillars as shown below.



As outlined above, each pillar constitutes several activities that should be carried out in order to effectively manage fraud risks. This policy defines the roles and responsibilities for various stakeholders for the program of activities set out in the FRM framework above.

The Board of Directors has the overall responsibility for overseeing the FRM program in the respective entities for which they have been appointed, under the Britam Group of Companies. They are responsible for approving, reviewing and monitoring compliance with the Policy. The Board may delegate this responsibility to the Board Audit Committee and/ or the Executive Committee.

Line Managers have the overall responsibility for implementing the FRM program under the leadership of their

respective CEOs and/or the Group MD. This would involve undertaking the fraud prevention, detection and response activities outlined above and discussed further in subsequent sections of this policy.

Group Forensics ("GF") is a section within the Internal Audit department with specialist fraud management expertise. They are responsible for providing guidance in relation to this policy and facilitating the implementation of this policy as outlined in the table below.

	Group MD, CEOs & Line Managers	Group Forensics (GF)
Fraud Prevention *Initiatives aimed at reducing the risk of fraud from occurring.*	• Set the tone at the top with regard to Britam's zero tolerance to fraud • Understand the FRM policy and cascade it together with other relevant communication to their teams. • Understand fraud risks that affect their respective functions • Establish relevant internal controls and measures to mitigate fraud risks.	• Develop relevant FRM policies & documentation • Coordinate fraud risk assessment exercises. • Coordinate communication & awareness initiatives. • Carry out fraud risk process reviews. • Provides regular reports to Management on the impact of frauds detected and measures taken to mitigate identified fraud risks.
Fraud Detection *Initiatives aimed at discovering fraud when it occurs*	• Implement adequate internal controls e.g. performing reconciliations. • Adequate supervision to ensure controls are effective. • Report all suspicions of fraud to GF	• Manage fraud reporting channels (hotline, email, direct reports etc.). • Suspicious transactions monitoring. • Maintain relevant black list information for referencing.
Fraud Response & Investigation *Initiatives aimed at taking corrective action and remedying the harm caused by fraud*	• Hold their teams accountable for compliance violations including taking appropriate remedial action • Support investigative efforts and provides relevant information, including carrying our necessary investigative procedures as directed by GF. • The Legal department will provide legal advice in relation to the outcome of investigations especially where court action is likely.	• Receive and consolidate all reports on fraud. • Carry out (or supervise) fraud investigations and report on findings. Investigation of theft cases will be carried out by the Security team. • Law enforcement liaison with the support of Legal and Security departments. • Submit relevant items of evidence to HR or Legal departments for use in disciplinary or court action as appropriate.

The rest of the Internal Audit department comprises Internal Auditors who will be required to include fraud risks in the scope of audit plans/cycle and highlight red flags where the Auditor believes a possibility of fraud exists.

All access persons are required to make themselves aware of this policy at all times, adhere to it, report all suspicions of fraud to GF or their respective Line Managers and to cooperate fully with investigations.

The FRM program will be independently reviewed from time to time by suitably qualified external consultants with a view to assess its effectiveness and provide recommendations on ways to enhance it. Where necessary, external support could also be sought for sensitive investigations or where appropriate investigative competencies that are not available in-house are required.

5.3 Examples and classification of fraud

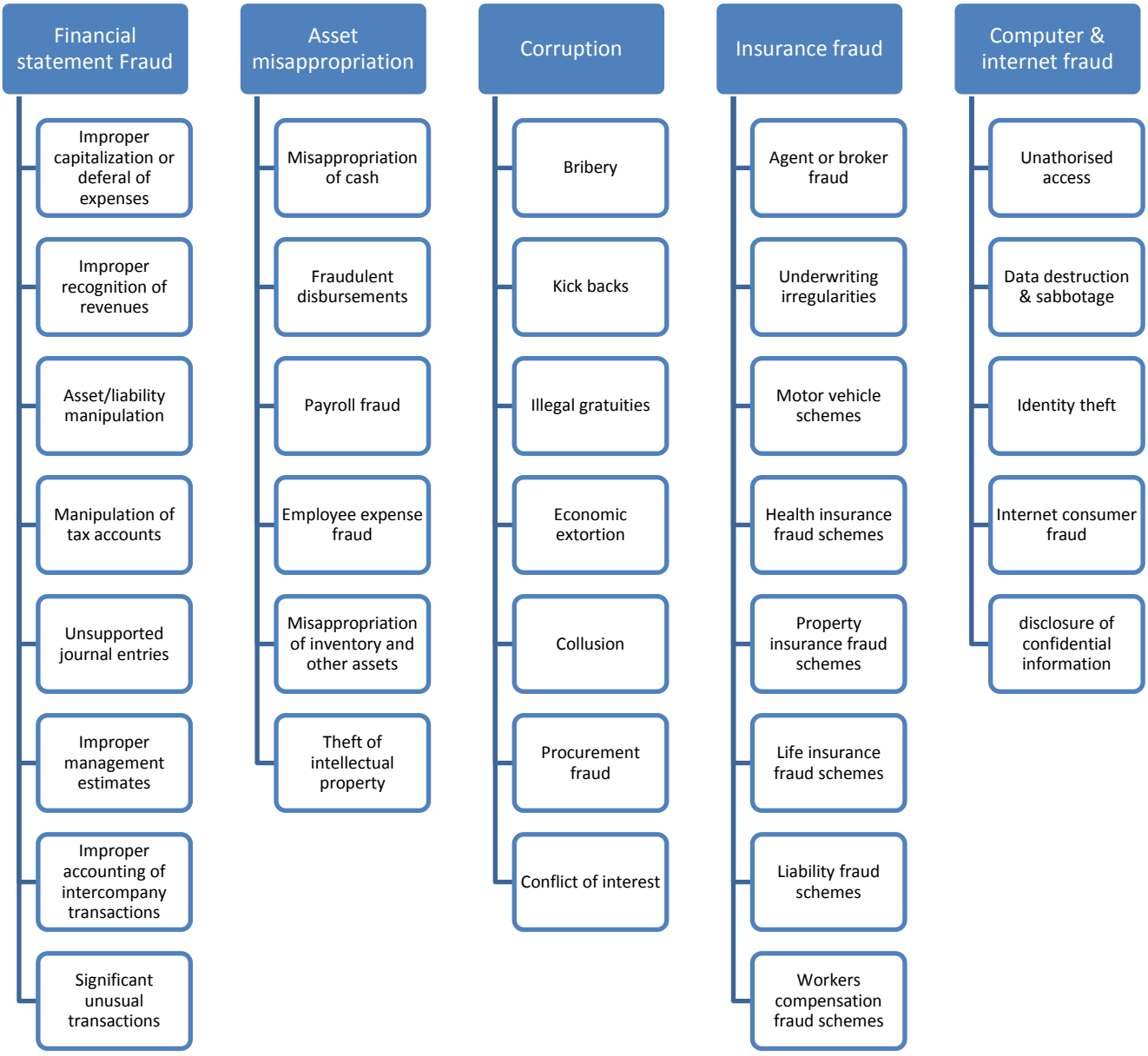
While fraudulent activity could have a very wide range of coverage, in the context of Britam, fraud includes (but is not limited to):

a) Forgery or unauthorized alteration of an application form or any document submitted by the customer.
b) Forgery or unauthorized alteration of any document or account belonging to the Company.
c) Forgery or unauthorized alteration of cheque, bank draft or any other financial instrument etc.
d) Misappropriation of funds, securities, supplies or others assets by fraudulent means etc.
e) Falsifying records such as pay-rolls, removing the documents from files and /or replacing it by a fraudulent note etc.
f) Making fraudulent or false representations.
g) Willful suppression of facts/deception (including concealment of errors) in matters of appointment, placements, submission of reports, etc. as a result of which a wrongful gain(s) is made to one and wrongful loss(s) is caused to the others.
h) Utilizing Company funds for personal purposes.
i) Authorizing or processing payments for goods not supplied or services not rendered.
j) Destruction, disposition, removal of records or any other assets of the Company with an ulterior motive to manipulate and misrepresent the facts so as to create suspicion/suppression/cheating and as a result of which objective decision would not be arrived at.
k) Dishonestly overstating or manipulating performance to enhance reward within employment.
l) Failure to report matters of fraud that come to your attention.
m) Any other act that falls under the definition of fraudulent activity as per the law.

The above characteristics form key elements of fraud in the insurance industry and could be classified into the following main categories:

a) Financial statement fraud – the deliberate misrepresentation of the financial condition of an enterprise accomplished through the intentional misstatement or omission of amounts or disclosures in the financial statements to deceive financial statement users.
b) Asset misappropriation – includes both the theft of company assets such as cash or inventory and the misuse of company assets such as using a company car for a personal trip.
c) Corruption - The offering, giving, soliciting or acceptance of an inducement or reward which may influence the action of any person.
d) Insurance fraud – occurs when people deceive an insurance company or agent to collect money to which they are not entitled; for instance, when the insurance company receives a misrepresented claim and the person submitting the misrepresented claim receives unwarranted benefits based upon the misrepresented information.
e) Computer fraud and internet fraud – refers to fraud perpetrated using a computer and the internet as the primary tool to commit fraud.

Outlined on the next page is a further breakdown showing broad of the types of fraud under each category:



5.4 Reporting channels

Britam encourages all access persons to escalate suspicions of fraud through the following channels that have been provided for:

#	**Reporting line**	**Contacts**
1	Line Manager	As per the Corporate Directory
2	Whistleblowing hotlines	As shown in the table below
3	Group Forensics Services (GF)	reportfraud@britam.com

**** All fraud incidents reported to the Line Manager must be ultimately reported to the GF*

Britam is committed to ensuring that there is a high level of privacy and confidentiality around the escalation of fraud incidents. In the course of investigations there may be need to refer to the reporting person for additional information or further clarification.

For those who wish to report anonymously, the whistleblowing facility is best suited for this. The whistleblowing facility contacts are set out below:

Reporting platform	Country	Whistleblowing hotline contacts
Toll free numbers	Kenya	0800724966
	Uganda	0800105060
	Tanzania	0800780072
	Mozambique	843203364
	Malawi	24247
	Rwanda	4252
Email Address	All	britam@whistleblowing.co.za
WhatsApp Number	All	+27 795 129 361

All reports received will be addressed appropriately through a suitable case management mechanism as outlined in section 5.5 below. This may involve GF working together with Line Manager to resolve reported cases.

5.5 Investigation and Response

5.5.1 Statement of Intent

Britam will maintain cost effective mechanisms that ensure suspected fraud is thoroughly and appropriately investigated, so that the Group, its Divisions and departments understand the impacts and root causes of all such events, and responds consistently to each issue as it arises.

5.5.2 Investigation Standard

All fraud investigations will be overseen the by GF. A case management system will be put in place that will classify all the fraud incidence reports received and GF shall develop the escalation criteria, response procedures and protocols depending on the type and scale of the fraud. Some cases may for instance be investigated by Line Managers under the supervision of GF while others may be investigated end to end by GF or the Security department.

Investigations will be concluded with a final report detailing the following:

- The allegations or areas of concern
- Inquiries undertaken
- Findings
- Conclusions
- Control improvements recommended

5.5.3 Investigation Objectives

A fraud investigation consists of gathering sufficient information to determine

- Whether fraud has occurred
- Who was involved
- The methods used to circumvent controls
- The loss or exposures arising

The investigation will be sensitive to the rights of individuals and will be conducted on an independent basis regardless of the suspected wrongdoer's length of service or position in the organization. The following key elements must be taken into account in undertaking an investigation:

- Confidentiality
- Maintaining the integrity of the investigator, ensuring no possible conflict of interest with the area being

investigated
- Evidence collection, preservation and presentation standards
- Documentation of the investigations steps and decisions taken

5.5.4 Periodic reporting of investigation findings

Britam considers a fraud event as significant when it meets any of the following criteria:

- Foreseeable net financial loss in excess of KES 1 million for Kenyan units or the equivalent of KES 500,000 for the regional units
- Extended reputation risk occurs (e.g. one-off adverse national media coverage, frequent or major impacts on customers or linked to a major external investigation)
- Severe legal and regulatory risk arises (e.g. a breach in regulations, or where a product is required to be withdrawn by the regulator and may include imposition of a fine).
- Any fraud investigation involving an employee who is graded above Manager; or is in a financial control (or controlled) position.

GF will report fraud incidences that meet the above criteria to the Group Board and Executive Council or its delegate Committees with relevant detail to understand the fraud schemes, including control gaps that contributed to the frauds. Incidences that do not meet the above criteria will be aggregated together and reported as part of overall fraud statistics.

Reports to the individual BU and Regional Boards will be made by GF.

5.6 Information Exchange with Regulatory or Statutory Authority

Where necessary, Britam shall share information on incidences of fraud as well as fraudsters with relevant authorities and industry bodies.

5.7 Review Cycle

This Policy will be reviewed annually by the Group Managing Director in conjunction with GF and any other stakeholders.

In the event that a new department or entity is established, this policy may undergo an unplanned review.

5.8 Related Policies and Procedures

This policy should we read in conjunction with the following:
- Incident Management Policy
- Incident Management Procedure
- Code of Business Conduct
- Whistleblowing Policy
- Anti-Money Laundering Policy
- Anti-Bribery and Corruption Policy
- Disciplinary Policy

5.9 Applicable Legislation & Regulations

- Provisions of local economic crimes legislation
- Provisions of local capital markets and Insurance legislation
- Any other related legislation in jurisdiction of Britam's operations

5.10 Related Forms and Guidelines

- Investigation Procedure
- Allegation sheet

- Investigation Report format
- Statements format