2023

Guidelines for Fraud Risk Management Framework in the Public Sector Entities,2023

The United Republic of Tanzania

Ministry of Finance

THE UNITED REPUBLIC OF TANZANIA
MINISTRY OF FINANCE

GUIDELINES FOR DEVELOPING AND IMPLEMENTING FRAUD RISK MANAGEMENT FRAMEWORK IN THE PUBLIC SECTOR ENTITIES

REVISED

JULY 2023

TABLE OF CONTENTS

STATEMENT OF THE PERMANENT SECRETARY

The Controller and Auditor General Report for the financial year 2020/21 show an increased risk of fraud including theft of assets, misappropriation of public funds and corruption in PSEs. Further, the Prevention and Combating of Corruption Bureau (PCCB) report, 2020 indicates increased risks of fraud in police force (17.9%), health sector (17.9%), courts of law (11.9) and revenue management (6.1%). On the other hand, the Association of Certified Fraud Examiners (ACFE, 2020) reported that 88% of fraud cases perpetrated against government entities have resulted median losses of TZS 800 million per annum. Such incidences lead to negative effects like tarnished image of PSEs, loss of stakeholders' confidence and poor service delivery. This therefore calls for concerted and coordinated efforts to curb such incidences, which according to CAG, 2021 are caused by cultural orientation, governance weakness, non-functioning of internal audit units culminating weak internal controls in PSEs.

The Government has taken number of measures to address the internal audit and internal control issues to minimize the risk of fraud in PSE. The Internal Auditor General Division was established in 2010 through amendment of Public Finance Act, CAP 348. Amongst the key responsibilities of the IAGD is to issue guidelines to improve the internal audit, internal controls and risk management in PSE. This has placed greater need for the Public Sector Entities (PSEs) to develop and implement their own risk management frameworks as part of their governance processes.

Consequently, Guidelines for Developing and Implementing Risk Management Frameworks in the Tanzanian PSEs were developed and issued in 2012. In the same line Guidelines for Developing and Implementing Fraud Risk Management Frameworks in the Tanzanian PSEs was developed in 2015. The Guidelines aimed at providing practical guidance to PSEs in developing and implementing customized fraud risk management frameworks.

However, since there has been changes in the way PSE operates including embedment of technology in service delivery, changes in international standards with regard to fraud risks and the issues related to risk of fraud observed in CAG report, has led to need for review and updating of the guidelines. The revised and updated Guidelines for Developing and Implementing Fraud Risk Management Frameworks in PSE, 2023 are expected to complement on the already designed and implemented enterprise risk management (ERM) systems in PSEs, and National Anti-Corruption Action Plan (NACAP).

It is a requirement, as part of the PSE governance improvement, that all PSEs should have robust fraud risk management policies, structures and procedures that will facilitate an effective assessment of fraud risks and strengthen fraud prevention organs as well as formulation of working policies to reduce fraud risks and thus improve public service delivery efficiency and effectiveness.

In developing these Guidelines, there were a lot of collaborative efforts. These involved close consultations amongst staff within the Internal Auditor General Division, Mzumbe University and other key stakeholders from both public and private sector. I wish to express my appreciation to all of them for their time and efforts in the successful completion of this document.

Mwamba

DR. NATU E. MWAMBA

PERMANENT SECRETARY –TREASURY

STATEMENT OF INTERNAL AUDITOR GENERAL

The review and updating of these guidelines is among the deliberate efforts geared towards enabling PSEs to provide quality and effective services to the public and reduce waste. It is on this premise that Section 32 of the Public Finance Act, CAP 348 gives Internal Auditor General with the responsibility to undertake continuous audit of risk management in the PSEs.

These updated Guidelines are composed of four sections:

- Introduction, Purpose, and Scope.
- Commitments and Implementation Guideline.
- Fraud Risk Management Guidelines to Public Sector Entities (PSEs); and
- Toolkit.

These sections provide practical guidance (steps and procedures) to PSE when developing and implementing their own customized fraud risk management frameworks. The Guidelines should be considered as a live document. They are subject to periodic review/ updates as and when significant changes in laws, regulations, standards occur and/or any other experience learned during the course of implementation that need to be captured in the document.

I stress on the key aspect that while developing and implementing the fraud risk management frameworks, PSEs should consider and align the frameworks with their current/ existing structures including frameworks for improving the internal control systems. Fraud risk management should not be treated same as enterprise risk management (ERM), but rather purely dealing with “fraud” in all functional areas of the PSE, thereby improve Internal Controls.

I also wish to record my appreciation to all individuals and organs that were involved in the process of preparation and finalization of these guidelines, for their dedication and commitment into the whole process. I furthermore, recognize the invaluable assistance, encouragement and support to the whole process by the Permanent Secretary - Treasury.

BENJAMIN M. MAGAI
INTERNAL AUDITOR GENERAL

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACFE	Association of Certified Fraud Examiners
AIAG	Assistant Internal Auditor General
AICPA	The American Institute of Certified Public Accountants
CAP	Chapter
CAG	Controller and Auditor General
CEO	Chief Executive Officer
CIMA	Chartered Institute of Management Accounting
COSO	Committee for Sponsoring Organizations of the Treadway Commission
ERM	Enterprise Risk Management
FRC	Fraud Risk Coordinator
FRO	Fraud Risk Officer
IAG	Internal Auditor General
IIA	The Institute of Internal Auditors
IRM	Institute of Risk Management
ISO	The International Organization for Standardization
LGAs	Local Government Authorities
MDAs	Ministries, Departments and Agencies
NACSAP	National Anti-Corruption Strategy and Action Plan
NBAA	National Board of Accountants and Auditors
PCCB	Prevention and Combating of Corruption Bureau
PSE	Public Sector Entities
RSs	Regional Secretariats

DEFINITIONS

Accounting Officer	Appointed officer by name and in writing by the Paymaster-General in respect of each expenditure vote, who controls and is accountable for the expenditure of money applied to that vote by an Appropriation Act and for all revenues and other public moneys received, held or disposed of, by or on account of the department or service for which the vote provides.
Corruption	The use of power, money or favors by people in position of authority or contacts in their network for illegitimate private gain.
Control	Any action taken by management, the governing board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.
Fraud	Any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.
Fraud Detection	Procedures to discover fraud during or after its occurrence
Fraud Deterrence	The process of eliminating factors that may cause fraud to occur
Fraud Prevention	Strategies that are designed to proactively reduce or eliminate fraud committed against an organization
Fraud Response	Plans and activities that take place after a fraud has been detected
Fraud Risk Assessment	A dynamic and iterative process for identifying, analyzing and evaluating fraud risks relevant to the PSEs.
Fraud Risk	It is a possibility of any unexpected loss, be it financial, reputational, or material, due to fraudulent activity by an internal or external intentional act or omission designed to deceive others to achieve a gain.
Fraud Risk Impact	The degree of loss or damage that would result from an occurrence of the fraud risk event.
Inherent Fraud Risk	Inherent risk is the initial risk that exists before any control is used to address or reduce the impact of that risk.
Fraud Risk Likelihood	A chance of fraud happening, whether defined, measured or determined objectively or subjectively, qualitatively, or quantitatively, and described using general terms or mathematically.

Fraud Residual Risk	Fraud risk remaining after fraud risk treatment. It is also known as "retained fraud risk".
Fraud Risk Analysis	The systematic process applied to determine the likelihood and impact on occurrence. It provides the basis for risk evaluation and decisions about risk treatment.
Fraud Risk Appetite	The amount of risk that an organization is prepared to accept (tolerate) or be exposed to at any point in time.
Fraud Risk Committee	An independent committee of the Board of Directors or a Management Committee (Depending on PSE Structure) that has, as its sole and exclusive function, responsibility for the oversight of the risk management policies and practices of the PSE's global operations and oversight of the operation of the Organization's overall risk management framework.
Fraud Risk Management Framework	Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing, and continually improving fraud risk management throughout the organization.
Fraud Risk Management Coordinator	A person appointed to coordinate issues of Fraud Risk Management in the PSEs.
Fraud Risk Management	A process that provides a framework to identify, analyze, evaluate, and treat fraud risks.
Fraud Risk Owner	The Senior Official responsible for the area that the fraud risk will impact on most or that has been assigned the responsibility for the fraud risk by his/her Accounting Officer.
Fraud Risk Register	A composite, prioritized, list of the identified and evaluated fraud risks outlining their likelihood and potential impact, and includes an action plan or proposed mitigating measures to manage or contain a fraud risk to acceptable Levels.
Fraud Investigation	A search or gathering of evidence relating to a specific fraud allegation(s) to determine the facts relating to the matter and to assist in deciding what, if any, action should be taken in relation to the matter(s).
Fraud Risk Tolerance	An organization or stakeholder's readiness to bear the fraud risk after the fraud risk has been treated, to achieve the organizations or stakeholder's objectives.

Public Sector Entity	All Tanzanian Public Sector Institutions: Ministries, Departments, Agencies, Parastatal Organizations, Public Corporations, Regulatory Authorities, Government Business Entities, Regional Secretariats and Local Government Authorities that are required to or expected to implement sound risk management systems.
Risk	The effect of uncertainty on objectives.
Tone at the top	An organization's general ethical climate and/or atmosphere, as established by its board of directors, audit committee, and senior management. Having a strong tone at the top is believed by business ethics experts to help prevent fraud and other unethical practices.

SECTION I

1 INTRODUCTION

This section covers introductory issues relating to fraud risk management which include introduction; definition and/or concepts of fraud, fraud risk and fraud risk management; legal context relating to fraud risk management in PSE as well as purpose, scope, structure, and review of the guidelines.

1.1 Background

Rise and increase of fraudulent activities in the Public Sector operation, result to less stakeholders' confidence, poor service delivery, demoralization of employees towards work performances just to mention a few. As such managing fraud risks calls for coordinated efforts within Public Sector Entities' (PSE s) with regard to its prevention, detection, and deterrence.

In this regard, PSE's managements must develop Fraud Risk Management Frameworks that assist fraud prevention and detection in a timely manner and create a strong fraud deterrence effect that promise meeting stakeholder's expectations, which include running efficient and effective operations, compliance with all applicable laws and regulations, meeting reporting and accountability responsibilities, and safeguarding resources that are entrusted to them.

The revision to the current version of the guide has considered the recent developments in the Fraud Risk Management practice for the Public Sector internally and globally. These includes Risk Management standards, technological changes, legal aspect, and experienced challenges by PSEs on the implementation of the existing Fraud Risk Managements on how to develop and their Fraud Risk Management Frameworks. The guidelines are revised so that it conforms to international standards on developing Fraud Risk Management Framework, mainly the COSO 2013, supplemented by ISO 31000:2018. However, efforts have been made to customize the procedure within the guidelines so that are generically applicable to all PSEs.

1.2 Fraud Regulatory Framework

The following are some legislations in United Republic of Tanzania which cover and/or highlight on issues relating to frauds:

i. *The Penal Code Act, CAP 16* – It is the main Act in relation to fraud. It provides several chapters relating to fraud i.e., Chapter X - Abuse of office (Sec. 94 to 96); Chapter XII – Section 120: frauds and breaches of trust by public officers; Section 270 – stealing by person in public service; Chapter XXXIII – fraud by trustees and persons in a position of trust and false accounting (Sect. 314-317); Chapter XXXIV – forgery including punishment Sec. 333,335 and 337.

ii. *The Prevention and Combating of Corruption Act, CAP 329* – Sections 23, 29, and 31 of the Act cover several issues relating to fraud. For instance, matters covered include use of documents intended to mislead principal; possession of unexplained properties, embezzlement and misappropriation of funds and transfer of proceeds of corruption (money laundering).

iii. *The Income Tax Act CAP* 332 – Section. 106 provides for offence of making false or misleading statement.

iv. *The Public Finance Act, CAP 348* - Section. 10 (3) of the Act covers issues which may render the public officer contribute to loss or deficiency of properties. Also, Part V: Losses, Sections 17 to 21 cover several actions to be taken against cash losses which include losses of cash by fraud and theft. For instance, stores losses; losses through claims or waivers, and losses through fruitless or nugatory expenditure. Similarly, Section 34 of the Act gives power to CAG to reveal and recommend to the Minister for Finance and Planning acts that relate to loss, negligence, carelessness, theft, dishonesty, frauds, and corruption relating to public resources.

v. *The Public Procurement Act, CAP. 410* – Section. 83 prohibits public officials and tenderers to engage themselves in frauds and /or corrupt practices. Also Sec. 104 provides for stringent sentences for offences i.e., giving false or misleading information, collusive or coercive acts geared towards committing frauds and corruption, and causing loss of public properties or funds as a result of negligence.

vi. *Sheria ya Maadili ya Viongozi wa Umma ya Mwaka 1995*- Sections 5 to 12 cover issues relating to ethical conduct and prohibitions of public leaders to use public office for personal gains and all other acts related to frauds.

vii. *Code of Ethics and Conduct for the* Public *Service issued under the Public Service Act, CAP 298* - covers for ethics and behavior expected of public servants in Tanzania.

viii. *Anti-money Laundering Act, CAP 423* – the act requires reporting person to report any issues of suspicious financial transactions, and conduct country risk assessment for money laundering and fraudulent transactions.

Based on these various requirements from various laws and regulations relating to fraud, the need for developing and implementing guidelines for fraud risk management in the PSEs is of necessity. The guidelines are meant for complementing the existing laws and regulations.

These guidelines are issued in line with Section 6 (2) of the Public Finance Act, CAP 348 which mandate the Permanent Secretary-Treasury to issue directions and/or instructions from time to time to ensure safe and efficient use of public resources i.e., *for the purposes of discharging the responsibility…the Permanent Secretary…may, subject to this Act, give any directions and instructions which he may consider necessary for safety, advantage, economy, and efficient use of public resources*.

The guidelines are also important aspect of public sector governance in PSEs, when responding to the current requirements of Section 6 (b) and 32 of the Public Finance Act, CAP 348 which gives the Internal Auditor General (IAG) the responsibilities to issue guidelines and ensure the effectiveness of risk management in PSE s including fraud risk management.

1.3 The Meaning of Fraud

Fraud is defined as:

> "*Any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.*"

(Source: COSO,2013)

Overall, it can be generalized that the term fraud involves activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery, and extortion.

There are generally three (3) key types/ categories of occupational frauds, namely:

i. *Asset misappropriation* – this involves theft or misuse of the PSE's assets e.g., theft of non-cash assets, false payments requests, false refund scheme, cheque fraud, payroll fraud, theft of motor vehicles, furniture's, inventory or cash, false invoicing, debtors' fraud, and payroll fraud.

ii. *Fraudulent financial statements* – normally in the form of falsification of financial statements with the intention of obtaining some form of improper benefits e.g., improper revenue recognition, recording fictitious sales, over /under estimating percentage of work completed on long term contracts, recording revenue or expenses in improper periods, manipulation of fixed assets valuations, falsification of documents such as employee credentials.

iii. *Corruption* - this includes activities such as illegal gratuity, extortion, bribery, use of bribes, or acceptance of "kickbacks"; improper use of confidential information conflicts of interest and collusive tendering.

1.4 Reasons for Committing fraud

There are mainly three (3) key reasons for frauds. They are summarized in the popularly known "the fraud triangle". The three elements are interrelated and must exist for fraud to occur.

Fraud Triangle, Fraud Deterrence & Internal Control

Of the three elements of a fraud triangle, removal of opportunity is most directly affected by the system of internal controls and generally provides the most actionable route to deterrence of fraud.

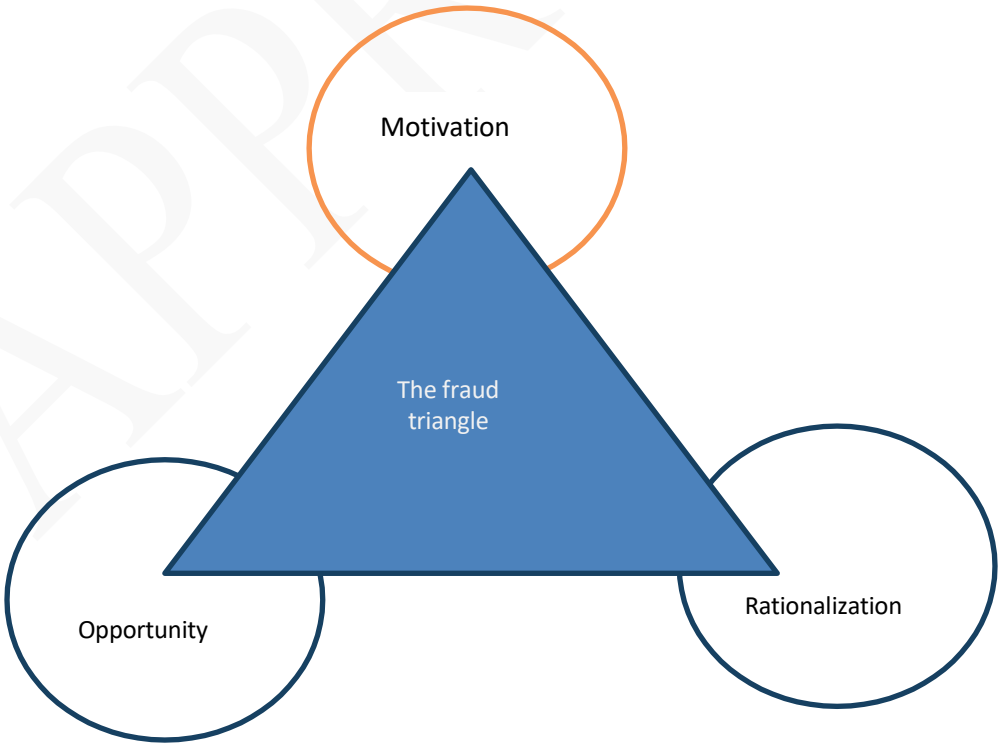
Handbook of Fraud Deterrence (2007)

i. *Motivation* – it is based on either selfishness desire for wealth i.e., greed or need. Majority of fraud cases are caused by greed and some due to problems arising from debts.

ii. *Opportunity* – especially in PSE where there is a weak internal control system, poor security over organizational property, little fear of exposure and likelihood of detection, or unclear policies with regard to acceptable behavior. Research has shown that although there could be some honest employees but given such opportunities there could be swayed away and fall into trap of committing frauds.

iii. *Rationalization*- based on the philosophy "if others are doing why not me". This occurs where there is inadequate or lack of legal enforcement.

Figure 1: The Fraud Triangle



1.5 Defining Fraud Risk and Fraud Risk Management

Fraud risk is defined as:

> *"Fraud risk is the vulnerability that PSE has in relation to the three* interrelated *elements that enable someone to commit fraud i.e., motive, opportunity and rationalization*."

Fraud risk management is defined as:

> *"Fraud risk management is a process that provides a framework to identify, analyze, evaluate, and treat fraud risks*."

Fraud risk management is an integral part of an anti-fraud program within the PSE.

1.6 Benefits of Managing Fraud Risks

Managing fraud risks in PSE s may include, among others, the following potential benefits:

i. Help in meeting regulatory requirements;

ii. Supplement the internal controls environment in helping to prevent, detect and deter fraud;

iii. Manage the impact of fraud on available funding;

iv. Protect the organization's resources;

v. Help address areas of exposure in PSE where the internal controls environment may have limitations such as collusion;

vi. Lead to improved efficiency and increased ability to meet commitments and /or PSEs objectives and performance targets;

vii. Creation of intact and enhanced image;

viii. Boost employee morale through job satisfaction and greater employment security; and

ix. Assure stakeholders' confidence.

1.7 Purpose of the Guidelines

The key purpose of the Guidelines is to provide guidance to PSEs in developing and implementing their Fraud Risk Management Frameworks.

Specifically, the guidelines serve the following purposes:

i. To disseminate the Government's commitment and intentions towards the adoption and implementation of fraud risk management practices across the public sector;

ii. To sensitize accounting officers, senior and all other staff of the PSE on the fraud risk management concept and its importance to PSEs;

iii. To provide insights on steps to be followed when developing and implementing customized fraud risk management frameworks;

iv. To provide a benchmarking criterion of evaluating internal and/or external capacity to develop and implement fraud risk management framework in the PSE;

v. To assist PSEs, embed fraud risk management culture and practices amongst all staff as well as put in place effective accountability strategies and mechanisms; and

vi. To assist internal auditors in providing independent assurance to the management, boards, oversight bodies an,d key stakeholders of PSE on the effectiveness of the fraud risk management frameworks.

1.8 Scope of the Guidelines

The scope of the Guidelines is focused primarily on providing generic guidance on commitment and approach to managing fraud risks. These guidelines apply to PSE as follows:

i. Across all levels of PSEs organizational structure activities and processes; and

ii. Restricted on fraud risk management and not fraud management which are covered by other legislations.

1.9 Structure of the Guidelines

The Guidelines are composed of four key sections as summarized in Table 1 below:

Table 1: Structure of the Guideline and Arrangement of Sections

SECTION	TITLE	DESCRIPTION
SECTION I	Introduction, Purpose, and Scope	Introduces the rationale for the government to commit itself to fraud risk management; describes the terms fraud, fraud risk , and fraud risk management; purpose and scope; structure and review of the guidelines.
SECTION II	Implementation requirements	Provides for the general government's commitment with regard to fraud risk management, adopted standard as well as implementation requirement and responsibilities.

SECTION III	Fraud Risk Management Guidelines to PSEs	Describes components of a Fraud Risk Management Framework. Also, discusses and/or describes detailed steps and procedures for developing, implementing, reporting and monitoring a fraud risk management framework.
SECTION IV	Template (Toolkit)	Provides for illustrations and the key templates for use in developing and implementing the fraud risk management framework.

1.10 Review of the Guidelines

The responsibility for updating the guidelines rests with the Internal Auditor General in line with Section 32 of the Public Finance Act, CAP 348.

The review should be after every five (5) years or when need arises in context of changes of international standards and governing laws.

SECTION II

2 IMPLEMENTATION REQUIREMENTS

This section covers purpose, commitment statements by the Government and adopted standards with regards to fraud risk management.

2.1 Purpose

The key purpose is to communicate the government's commitment to PSEs and all other relevant stakeholders working with PSEs in one way or another. It is also aimed at charging PSE officials with responsibilities for effective fraud risk management in their areas of responsibilities.

2.2 Government's Commitment on Fraud Risk Management

The Government recognizes that fraud has been and continues to be an increasing risk in the PSEs. As such it poses challenges to PSEs with regard to its prevention and detection. Therefore, the management of fraud risks is an integral part of sound public sector governance and must supplement the internal controls environment by helping to prevent, detect and deter fraud. This in turn leads to improved efficiency and increased ability to meet commitments and /or organizational objectives and performance targets as well as increased stakeholders' confidence

The Government is committed to institute (i.e., develop, adopt and implement) a sound and effective fraud control across the public sector through the Ministry of Finance and Planning. It takes an active role in providing and setting broad guidance and support on the development and implementation of fraud risk management practices across the public sector. With the same commitment, the Accounting Officers of all PSEs are charged with the responsibilities of developing, adopting, and implementing effective fraud risk management practices in their organizations.

2.3 Adoption of Fraud Risk Management Standards

Fraud risk management builds on internal control and enterprise risk management (ERM) models. In these guidelines therefore, the fraud risk management is in accordance with the COSO 2013, and rthe isk assessment process complies with ISO 31000:2018 which has also already been adopted in the Guidelines for Developing and Implementing Institutional Risk Management Framework in the Public Sector issued by the Ministry of Finance and Planning, 2023.

Thus, the fraud risk management framework follows the same steps and in the same sequence as those of Enterprise Risk Management (ERM).

2.4 Implementation Requirements

Each Accounting Officer of the PSE is required to develop, and implement a fraud risk management framework. Accounting Officers of PSEs are required to ensure that:

i. Personnel throughout the PSEs are aware of fraud risk management policy including the type of fraud and misconduct that may occur;

ii. There is a policy, culture, and structure that facilitates how the PSE will identify record and monitor fraud risks, including procedures for reporting fraud risks information to the oversight organs;

iii. There is a fraud risk management process which is in line with international standards for risk management under ISO 31000;

iv. The fraud risk management process is part and parcel of the overall enterprise risk management within the PSE;

v. There is a fraud risk register that is used to record, rate, monitor and report fraud risks; and

vi. There is an established process for monitoring, reviewing, and enhancing fraud risk management and governance systems.

2.5 Implementation Responsibilities

The implementation responsibility of these guidelines is placed to all accounting officers (at the centre) and institutional level for various executive authorities and officials in PSEs.

However, at an institutional level, all PSEs need to customize the specific roles and responsibilities so that they align to their organizations' structure and context. Detailed implementation responsibilities are provided under Section III of these Guidelines.

SECTION III

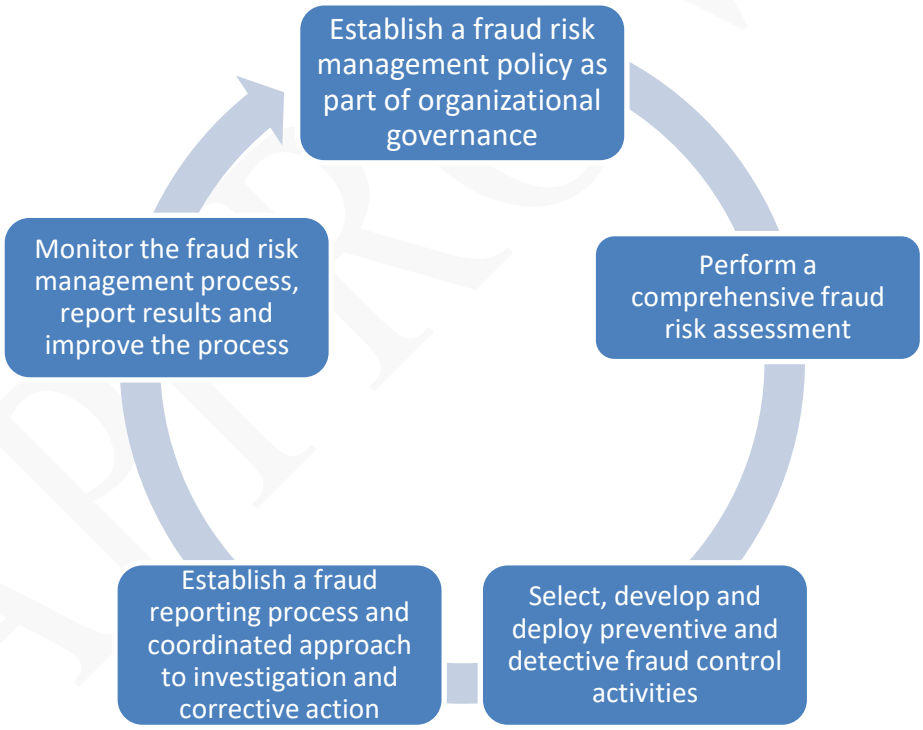
3 FRAUD RISK MANAGEMENT GUIDELINES

This section provides guidance to the process of developing and implementing the PSE's fraud risk management framework.

The section outlines the key components of a fraud risk management framework and the detailed steps including how to conduct a fraud risk assessment process leading to the identification and assessment of fraud risks and the development of a fraud risk register and fraud risk treatment action-plans.

Figure 2 below summarizes the steps:

Figure 2: Overall Fraud Risk Management Framework



3.1 Principles of Fraud Risk Management

Fraud risk management is a framework explained within the five (5) key principles regarding managing fraud risks[1].

i. *Principle 1 – Fraud Risk Governance*: The PSE establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors/highest governance authority and senior management with their commitment to high integrity and ethical values regarding managing fraud risk.

ii. *Principle 2 – Fraud Risk Assessment*: The PSE 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.

Components of Fraud Risk Program:

The five key [principles] components of a comprehensive fraud risk management program/ framework are: (1) fraud risk governance, (2) fraud risk assessment, (3) fraud control activities, (4) fraud investigation and corrective action, and (5) fraud risk management monitoring activities.

Source: Alvarez & Marsal (2022)

iii. *Principle 3 – Fraud Control Activities*: The PSE 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.

iv. *Principle 4 – Fraud Investigation and Corrective Action*: The PSE 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.

v. *Principle 5 – Fraud Risk Management Monitoring Activities*: The PSE 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 above principles should be used as components formulating and documenting comprehensive fraud risk management program.

The following sub-sections give a detailed guidance on how to implement each of the above five key principles

[1] COSO/ACFE (2016) – Fraud Risk Management Guide.

3.2 Establish Fraud Risk Governance

PSEs must establish effective governance processes which are foundation of fraud risk management.

Fraud risk governance includes all aspects that set supportive internal environment for fraud risk management process to effectively take place.

Principle 1: Fraud risk governance

The PSE 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.

COSO/ACFE (2016)

3.2.1 Set High Level Commitment to Fraud Risk Management

Strong leadership sets a key foundation towards supporting an effective fraud control within the PSE.

This sets the "tone at the top" which implies:

a) Leaders/ managers are required to demonstrate an observably high level of commitment to the control of fraud through effective PSEs governance structure, with clearly defined roles and accountabilities for individuals and decision-making bodies (e.g., Board/Council, Audit Committee, Executive Management, Operational Management etc.);

b) There should be a "top- down" and "bottom-up" approach to fraud control which will ensure consistency and mutual reinforcing for managing frauds through the laid down organization's policies, governance structures and processes;

c) The board of directors/highest governance authority (where applicable) should ensure that its own governance practices set the tone for fraud risk management and that management implements policies that encourage ethical behaviors, including processes for employees, customers, service providers, and other third parties to report instances where those standards are not met;

d) The Board and top management should monitor the PSE's fraud risk management effectiveness, which should be a regular item on its agenda; and

e) To this end, the board (where applicable) or highest governance authority should appoint one executive- level member of management to be responsible for coordinating fraud risk management and reporting to the board or accounting officer on the topic.

3.2.2 Establish Fraud Risk Governance Roles and Responsibilities

PSE should ensure that there are defined roles and responsibilities with regard to fraud risk management, and everyone has to be aware of individuals and collective fraud risk management responsibilities.

a) While all employees are responsible for maintaining an environment of ethical behavior and intolerance to fraud, specific responsibilities and duties need to be clearly defined and assigned;

b) PSE should assign the overall responsibility for fraud risk management to a single executive-level individual who reports either to the Board/ Audit Committee or to the Accounting Officer as the situation may dictate;

c) Depending on the structure of PSE, design a fraud risk governance structure that defines appropriate fraud risk management roles and responsibilities of officials and all staff, e.g.:

    a. The Board/Council / Permanent Secretary (where applicable);
    b. Accounting Officer;
    c. Fraud Risk Management Committee;
    d. Audit Committee;
    e. Executive Management;
    f. Fraud Risk Coordinator;
    g. Fraud Risk owners;
    h. Risk Management Champions; and
    i. Other staff, contractors, and stakeholders.

d) The fraud risk governance structure can be represented diagrammatically as a means of identifying the committees and officials with fraud risk management responsibilities and the relationships between those committees and officials;

e) PSEs should appoint a Fraud Risk Coordinator to take up overall responsibility for maintaining the fraud risk management framework and for coordinating the work of other functions involved in fraud control matters. The Fraud Risk Coordinator and all other staff should:

    a. Have a basic understanding of fraud and be aware of the red flags;
    b. Understand their roles within the internal control framework;

c. Read and understand policies and procedures (e.g., the fraud policy, code of conduct, and whistleblower policy), as well as other operational policies and procedures, such as procurement manuals;

d. As required participate in the process of creating a strong control environment and designing and implementing fraud control activities, as well as participate in monitoring activities;

e. Report suspicious or incidences of fraud; and

f. Cooperate in investigations.

The tentative roles and responsibilities of the key players in the Fraud Risk Management is detailed under the following part.

3.2.2.1 Governing Boards/Councils

Where applicable, and depending on the structure of the PSE, the Board/Council other Higher Authority provides direction and oversight of fraud risk management across the organization.

The board's key fraud risk management responsibilities may include:

i. Approving the PSE's fraud risk management documentation (fraud risk management policy, plans, structure, procedures and fraud risk registers) which ensures ethical behaviour.

ii. Setting the standards and expectations of the organization with respect to conduct and behavior, and ensuring the effective fraud risk management is enforced through an effective performance management system.

iii. Establishing and communicating an appropriate level of fraud risk tolerance for the PSE

iv. Monitoring the management of high and significant fraud risks, policies and the effectiveness of associated controls through the review and discussion of semi-annually fraud risk management reports.

v. Satisfying itself that fraud risks with lower ratings are effectively managed, with appropriate controls in place and effective reporting structures.

vi. Approving major decisions affecting the organization's fraud risk profile or exposure

3.2.2.2 Accounting Officers

Accounting Officers are accountable for the overall governance of the fraud risk management practice in the PSE. They will oversee the development and implementation of fraud risk management frameworks that align to their PSE's operations, structure and context.

Specifically, the Accounting Officers have the responsibility to:

i. Setting an appropriate tone by supporting the adoption and implementation of effective fraud risk management.

ii. Design, implementation, and enhancement of fraud risk management framework.

iii. Delegate responsibilities for fraud risk management to fraud risk management and internal formations so that it aligns to the existing PSE structure, processes, culture and context.

iv. Ensuring appropriate action in respect of the recommendations of audit committee, internal audit, and external audit with regard to issues of fraud risk management.

v. Providing assurance to relevant stakeholders that key fraud risks are properly identified, assessed and mitigated.

3.2.2.3 Audit Committee

Depending on the reporting structure of the PSE, there are some PSE which have a risk management committee in place, while others have not. It is here advised that if theresn't a special committee for risk management, there is no need to form one at the early stages of adopting fraud risk management. Instead, the audit committee should be given the responsibilities for this aspect by including issues of both enterprise and fraud risk management in its existing charter.

Also depending on the nature of the PSE, where some have Audit Committee/or a risk management committee as committees of the governing board/of council, hence is more of an oversight than advisory. It is advised that the roles and responsibilities should be designed to fit this structure. However, as in most PSEs, the Audit Committee has an advisory role and reports to the Accounting Officer.

In relation to fraud risk management, the Audit Committee should therefore:

i. Play active role in the oversight of the fraud risk assessment

ii. Familiarize itself with fraud risk management process and approach of the organization.

iii. Catalyze risk management by enquiring from management risk assessments and treatment reports.

iv. Ask to see the departmental/ institutional level fraud risk registers periodically.

v. Review all matters related to fraud risk and risk management, through fraud risk management reports, on the manner they are being managed through use of internal and external audit reports

vi. Ensure appropriate internal audit work is undertaken with regards to fraud risks, by ensuring that internal audit plans are risk-based and focus on the most significant risk areas (ERM and fraud).

vii. Provide regular feedback to the Accounting Officer/ the Board/Council on the adequacy and effectiveness of fraud risk management in the PSE, including recommendations for improvement.

3.2.2.4 Fraud Risk Coordinator

There shall be a fraud risk coordinator (FRC), who shall be appointed to coordinate issues of fraud risk management in the PSE. For PSEs with mature risk management practices, the officer is also named as the Fraud Risk Officer (FRO). This officer is also a primary fraud risk champion. The FRC, works to assisting the Accounting Officer, and is therefore responsible for coordinating efforts in designing the PSE's fraud risk management framework and for the day-to-day activities associated with coordinating, maintaining and embedding the framework in the organization.

At the beginning, it is recommended that the Risk Management Coordinator of the PSE in respect of the Enterprise Risk Management activities be also assigned the coordinating role of issues relating to fraud risk management. However, as systems and activities relating to risk management and as well as fraud risk management expand, a specific Fraud Risk Coordinator may be appointed. For that matter, it is recommended that a staff member who has operational responsibility in human resources, legal or accounting & finance can be assigned the role of a fraud risk coordinator. In some circumstances, for example in smaller PSEs, or when adopting fraud risk management for the first time, the Chief Internal Auditor or Head of Audit Unit may fulfill this role. However, if the Chief Internal Auditor is given this role, appropriate safeguards must also be put in place to address the threats to independence of both roles.

Specifically, the role of the FRC is to assist the Accounting Officer to fulfill his/her fraud risk management roles. The fraud risk coordinator has the responsibility to:

i. Coordinate efforts for developing and implementing appropriate fraud risk management policies, procedures and systems.

ii. Co-ordinate and monitor the implementation of fraud risk management initiatives within an organization.

iii. Work with fraud risk owners to ensure that the fraud risk management processes are implemented in accordance with agreed fraud risk management policy and strategy.

iv. Collate and review all fraud risk registers for consistency and completeness.

v. Provide advice and tools to staff, management the Executive and Board on fraud risk management issues within the organization, including facilitating workshops in fraud risk identification.

vi. Promote understanding of and support for fraud risk management including delivery of fraud risk management training.

vii. Oversee and update organization-wide fraud risk profiles, with input from fraud risk owners.

viii. Ensure that relevant fraud risk information is reported and escalated or cascaded, as the case may be, in a timely manner that supports organizational requirements.

ix. Attend at audit committee meetings where fraud risk management issues are discussed.

3.2.2.5 Directors, Head of Divisions/Departments, Units and Sections (Fraud Risk Owners)

Also depending on the structure of a PSE, line managers, or functional specialists are the ones who assume responsibility for designing, implementing, and/or monitoring fraud risk treatments. These are also termed as Fraud Risk Owners, who are responsible for the following:

i. Design and implementation of a fraud risk management program
ii. Implementing and documenting a fraud risk assessment process
iii. Maintaining adequate documentation of design of antifraud programs and controls
iv. Evaluating design and operating effectiveness of antifraud programs and controls
v. Reporting to the Accounting Officer (through Fraud Risk Coordinator) on actions that have been taken to manage fraud risks and the effectiveness of the fraud risk management program
vi. Educating the organization on areas of potential compliance violations
vii. Enforcing Code of Ethics.
viii. viii. Provide information about the frau risk when it is requested. This includes giving cooperation to auditors (both internal and external) in the course of audit of fraud risk management activities within their departments or directorates
ix. Preparation of quarterly fraud risk management implementation reports of fraud risk treatment action plans and to submit them to the Fraud Risk Coordinator.
x. Annual review of their fraud risk registers and related controls.
xi. Maintenance of fraud risk register and other documents/ reports relating to risk management within their respective departments or directorates in a systematic manner.

3.2.2.6 Risk Champions

It is advised where in the PSE there are already existing risk champions, the same should be used for championing fraud risk management i.e. working together with the Fraud Risk Coordinator to promote fraud risk management across the PSE, or specifically within a particular function or project. They can help embed fraud risk management into the PSE other systems and processes. Champions can also help ensure that functional and project areas are using the entity's fraud risk management processes consistently.

A risk champion may hold any position within the entity, but is generally a person who:

i. Has the skills, knowledge and leadership qualities required to support and drive a particular aspect of risk management (both ERM and fraud).

ii. Has sufficient authority to intervene in instances where fraud risk management efforts are being hampered by a lack of cooperation or through lack of risk management capability or maturity.

iii. Is able to add value to the fraud risk management process by providing guidance and support in managing difficult fraud risk or fraud risks spread across functional areas.

3.2.2.7 Internal Audit

The Internal Audit Unit/ Department has the responsibility to provide overall assurance and advice to the Accounting Officer by conducting the following activities:

i. Evaluating the effectiveness of the fraud risk management activities in ensuring that key fraud risks facing the PSE are being managed appropriately.

ii. Provide assurance to the Board/ Council and to management that existing controls are appropriate given the fraud risk tolerance established by the Board/ Council

iii. Consider fraud risks when developing annual audit plan and spend time to evaluate the design and operation of antifraud controls

iv. Auditing the adequacy of fraud risk management process.

v. Providing active support and involvement in the fraud risk management process such as:

   a. Championing and coordination the adoption of fraud risk management practices (at the initial stages where there is no a fraud risk coordinator).

   b. Participation in audit committee meetings where fraud risk management issues are discussed. Hence, provide support to the audit committee in performing detective activities around the risk of management override of control

   c. Monitoring activities and status reporting.

   d. Training and education of front-line staff in fraud risk management and internal control including areas of potential fraud and compliance violations

   e. Facilitating fraud risk workshops.

   f. Internal auditors should pay particular attention on the professional limitation of their role with regard to fraud risk management activities. This should be made in reference to IIA position statement (i.e., on core roles, legitimate roles and roles not to undertake).

3.2.2.8 . All Staff

i. It is the responsibility of all personnel, stakeholders and contractors to apply the fraud risk management process to their respective roles. Their focus should be upon:

ii. Having basic understanding of fraud and awareness of red flags

iii. Reading and understanding policies and procedures on frauds (. e.g. fraud policy, code of conduct, conflict of interest policy, whistleblower policy etc.)

iv. Participating in the process of creating a strong control environment

v. Identifying fraud risks and reporting these to the relevant risk owner(s). Where possible and appropriate, they should also manage these risks.

vi. Reporting suspicions or incidences of fraud and corruption

vii. Cooperating with investigators

3.2.3 Formulate a Fraud Risk Management Policy

The PSE should have written policies and procedures to manage fraud risk representing a fraud risk management program as detailed hereunder:

a) Formulation of the fraud risk policy should clearly put the PSE's commitment on fraud risk management. Above all, the fraud risk policy assists employees to understand what fraud is, their PSE's attitude to fraud and their responsibility in relation to fraud incidences;

b) The formulated Fraud Risk Management Policy should clearly define fraud, identify both internal and external potential perpetrators of fraud, provide hypothetical organizational-based examples of fraud, and define the roles and responsibilities of those charged with oversight of fraud control;

c) The following elements must be included in the policy document:

   a. The policy should be comprehensive to include processes and procedures for managing fraud risks in the PSE.

   b. The Fraud Risk Management Policy should articulate risk tolerance considerations and expectations that suspected frau will be reported immediately.

   c. The main content of the policy may be organized by chapters or sections as exemplified under Template 1.

3.2.4 Document the Fraud Risk Management Program/ Framework

The PSE should document all the above aspects into a document that will be termed as Fraud Risk Management Framework[2].

[2] Interchangeably used as Fraud risk management program.

a) The documented Fraud Risk Management Program, including the fraud risk management policy should be documented and updated based on the PSE's current risk profile and experience; and

b) The documented framework should be endorsed by Board or the Accounting Officer or higher authority within the PSE, reissued periodically, and tracked to ensure receipt and understanding by all stakeholders.

Template 2 provides a sample of the Fraud Risk Management Framework.

3.2.5 Communicate the Fraud Risk Management Framework

The PSE fraud risk management framework, especially the policy must be communicated to both internal (and relevant external) stakeholders based on the following premises:

a) The aim for such communication is to make sure that all personnel and stakeholders understand their expectations related to the PSE's fraud risk management policy;

b) It also serves to raise awareness on its presence and specific requirements. This will enhance compliance and application of stipulated procedures;

c) The documented framework should be included in training course which should be mandatory for all employees; and

d) There is a number of ways in which the framework can be communicated to stakeholders, including meetings, workshops arranged for the purpose, fliers, and making it available on the PSE website or repository for reference when needed.

3.3 Assess the Risk of Fraud

Fraud risk assessment is a process aimed at proactively identifying and addressing an PSEs vulnerability to internal and external fraud. It is an ongoing and continuous process.

- The Fraud Risk Assessment process in PSE should comply with the requirement of risk assessment provided under PSE's Risk Management Framework.

- The Guidelines for Developing and Implementing Risk Management Framework in Public Sector should be read for detailed reference.

Principle 2: Fraud risk assessment

The PSE 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.

COSO/ACFE (2016)

3.3.1 Involve Appropriate Levels of Management

Management, including senior management, Unit/Section Heads, and significant process owners (e.g., engineering, legal, accounting, sales, procurement, and operations) should participate in the assessment, as they are ultimately accountable for the effectiveness of the PSE's fraud risk management efforts.

3.3.2 Form a Cross-departmental Fraud Risk Assessment Team

PSE Management should identify competent individuals to form a Fraud Risk Assessment Team.

This team should include individuals throughout the PSE with different knowledge, skills, and perspectives.

The team should include a combination of internal staff/ official and/ or external stakeholders (if necessary) such as:

a) Accounting/finance personnel who are familiar with the financial reporting and internal control;

b) Non-financial units and operations personnel to leverage their knowledge of day-to-day operations;

c) Customer and vendor interactions and general awareness of issues within the industry;

d) Risk management personnel, to ensure fraud risk assessment process integrates with the Risk management program;

e) Legal and compliance personnel, as fraud risk assessment will identify risks that give rise to potential criminal, civil, and regulatory liability if the fraud or misconduct were to occur; and

f) Internal audit personnel, who will be familiar with the PSE's internal controls and monitoring functions. In addition, internal auditors will be integral in developing and executing

responses to significant risks that cannot be mitigated practically by preventive and detective controls.

If the expertise is not available internally, external consultants with expertise in applicable standards, key risk indicator, anti-fraud methodology, control activities, and detection procedures should be engaged.

3.3.3 Decide on Criteria for Measuring and Tolerance of Fraud Risk

Any risk is measured using two dimensions, namely: likelihood of happening and impact once it happens. The product of impact and likelihood facilitates the comparison of fraud risks based on risk tolerance levels, and the overall risk appetite of the PSE.

Both the evaluation of likelihood and impact of (significance) of identified fraud risks may base on historical information, known fraud schemes, and interviews with process owners.

The criteria and rating scales for estimating the likelihood and impact for fraud risk must be consistent with those used for enterprise risk management as stipulated in the PSE's Risk Management Framework.

i. Likelihood of fraud risk

Likelihood represents the possibility that a given event will occur. The likelihood of a fraud risk may be assessed using two scenarios, either:

- Basing on the annual *frequency* of happening, or
- Basing on judgement of *possibility* of happening.

The evaluation of the likelihood may base on instances on which the fraud has occurred in the PSE in the past, the prevalence of the particular fraud in the sector, and other factors.

Table 2 provides and illustration for the scales and criteria for assessing the likelihood of a risk happening.

Table 2: Illustrative 5-point Scale Likelihood of Risk (COSO, 2012)

Rating	Annual Frequency		Probability	
	Descriptor	***Definition***	***Descriptor***	***Definition***
5	Frequent (Very High)	Up to once in 2 years or more.	Almost certain	90% or greater chance of occurrence over life of asset or project.
4	Likely (High)	Once in 2 years up to once in 25 years.	Likely	65% up to 90% chance of occurrence over life of asset or project.

Rating	Annual Frequency		Probability	
	Descriptor	***Definition***	***Descriptor***	***Definition***
3	Possible (Moderate)	Once in 25 years up to once in 50 years.	Possible	35% up to 65% chance of occurrence over life of asset or project.
2	Unlikely (Low)	Once in 50 years up to once in 100 years.	Unlikely	10% up to 35% chance of occurrence over life of asset or project.
1	Rare (Very Low)	Once in 100 years or less.	Rare	<10% chance of occurrence over life of asset or project.

ii. Impact (or Significance) of Fraud Risk

Impact refers to the extent to which a risk event might affect the PSE in terms of financial, reputational, regulatory, health, safety, security, environmental, employee, customer, and operational impacts. PSE should assess the significance of a fraud risk by considering financial and monetary significance as well as significance to the PSE's operations, brand value, reputation, and criminal, civil, and regulatory liability.

Table 3 provides an illustrative scales and criteria for judging the impact of a risk for a 5-point scale.

Table 3: Illustrative 5-point Scale for Assessing Impact of a Risk (COSO, 2012)

Rating	Descriptor/ color	Definition
5	Extreme (Very High)	• Financial loss of TZS X million or more[3]. • International long-term negative media coverage; game-changing loss of market share • Significant prosecution and fines, litigation including class actions, incarceration of leadership • Multiple senior leaders leave.
4	Major (High)	• Financial loss of TZS X million up to TZS X million

[3] Financial impact is typically measured in terms of loss or gain, profitability or earnings, or capital. This measure varies from PSE to PSE depending on their financial materiality.

Rating	Descriptor/ color	Definition
		• National long-term negative media coverage; significant loss of market share • Report to regulator requiring major project for corrective action • Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice.
3	Moderate	• Financial loss of TZS X million up to TZS X million • National short-term negative media coverage • Report of breach to regulator with immediate correction to be implemented • Widespread staff morale problems and high turnover
2	Minor (Low)	• Financial loss of Tshs X million up to Tshs X million • Local reputational damage • Reportable incident to regulator, no follow up • General staff morale problems and increase in turnover
1	Incidental (Very Low)	• Financial loss up to Tshs X million • Local media attention quickly remedied • Not reportable to regulator • Isolated staff dissatisfaction.

iii. Fraud risk tolerance levels

Fraud risk tolerance levels determine the amount (and type) of fraud risk that a PSE may or may not take relative to its objectives.

As pointed out earlier, to tolerate a fraud risk DOES NOT MEAN that the PSE regards the risk as negligible, rather as something that need to be kept under review and/or seek possibilities to reduce the fraud risk further, where possible[4].

[4] Most PSEs have a "zero" appetite to the risk of fraud, hence limiting the tolerance level of fraud risk to the red region of their risk heatmaps.

When risk rate is used for setting the fraud risk tolerance level, a PSE may draw a Fraud Risk Heat Map and determine in which region each fraud risk falls.

Table 4 to provides areas/ groupings of risk rates and levels of risk tolerance as result of multiplying the fraud risk impact and likelihood.

Table 4: Risk Ratings and Color Status to Guide Risk Tolerance Levels

Risk Rate (Impact x Likelihood)	Description	Risk Tolerance	Meaning and Responses
15-25	Extreme or severe	**NoTolerance (Unacceptable)**	Very serious concern; highest priority. Take immediate action and review regularly.
10-14	High	**Cautious** *"OK to proceed, but only if the likelihood and consequence of the fraud risk can be managed at reasonable cost".*	Serious concern; higher priority. Take immediate action and review at least three times a year
5-9	Moderate	**Tolerable / Conservative** *"OK to proceed, providing that losses and damage can be minimized".*	Moderate concern: steady improvement needed. Possibly review biannually
1-4	Low	**Acceptable** *"OK to proceed, even if ability to minimize potential losses is limited".*	Low concern; occasional monitoring. Tolerate/ Accept. Continue with existing measures and review annually.

3.3.4 Identify Fraud Risks in each Area of the PSE

Fraud risk identification involves gathering information to obtain the population of fraud risks that could apply to the PSE. The objective of fraud risk identification is to generate a comprehensive

list of fraud risks based on those events and circumstances that might affect the operations of the PSE.

The following sub-sections give detailed procedures:

i. Consider All Areas of the PSE

Unlike a normal risk identification which start with risks inherent in objective/ targets, fraud risk identification focuses on "fraud risk inherent in key areas/ operation of the PSE activities".

The risk assessment team should engage in a brainstorming session/ workshop to identify:

a) Incentives, pressure, and opportunities to commit fraud;

b) The risk of management override of controls; and

c) The fraud risk that are most relevant to the PSE.

ii. Consider Various Types of Fraud

Identification of fraud risk makes consideration of all types of fraud, including:

a) Fraudulent financial reporting, fraudulent non-financial reporting, misappropriation of assets, and illegal acts such as corruption;

b) The identification should consideration of fraud schemes and scenario, incentives, pressure, and opportunities to commit fraud, and IT fraud risks specific to PSE; and

c) The identification should also consider aspects of what, where, when, why, and how fraud could happen.

Template 3 provides examples of common fraud risk categories, schemes, and scenarios.

iii. Document the Identified risk in a fraud identification and analysis sheet

a) The team should, at first produce a list of fraud risks on each area/ activity that they worked on;

b) This list should be discussed with the members of the workshop or stakeholders before documenting them in a specially formulated sheet for further analysis;

c) Template 4 provides are sample of Fraud Risk Identification and Analysis Sheet to be used for documenting and analysis of agreed fraud risks;

d) Each fraud risk shall be documented individually in its own sheet;

e) The sheet shall be used to document the following aspects of the fraud risk assessment:

a. the identified fraud risks;

b. the causes of the risk

c. the impact and likelihood of the fraud risk (both inherent and residual);

d. existing controls against the respective fraud risks;

e. weaknesses observed in existing control against the fraud risks; and

f. proposed mitigations to be taken against fraud risks.

3.3.5 Estimate the Likelihood and Impact of Inherent Fraud Risk

The term *inherent fraud risk* means is a risk of fraud before the PSE has taken any action to mitigate the fraud risk.

a) This is mostly based on the assumption that there are no mitigating controls put in place against potential frauds on the area being assessed;

b) Although this might, sometimes be hypothetical, the idea for doing this is for the team to be able to appreciate the "seriousness" of the fraud risk in the area when controls are not working; and

c) In estimating the rate of inherent fraud risk rate, the team should use the risk measurement criteria established (see Section 3.3.3), which must also be consistent with the PSE's Risk Management Framework.

3.3.6 Identify and Document of Key Existing Control Activities and their Weaknesses

The role of existing controls is to reduce the *inherent fraud risk* into an acceptable level (as compared to the PSE tolerance levels).

Therefore, it is a good idea to document them and appraise their effectiveness and have a basis for proposing improvement on the area.

After all relevant inherent fraud risks have been identified and rated, the team should now:

a) Identify and document key control activities placed against the identified fraud risks.

b) Assess effectiveness of existing controls and document weaknesses in those controls.

Template 4 provides a specific area for documenting the existing controls and observed weaknesses.

3.3.7 Rate the Residual Fraud Risk and Compare with the Tolerable Levels

Residual fraud risk is the amount of fraud risk that remains after considering the effectiveness of existing controls/ mitigations against the respective fraud risk.

The logic for amount of residual fraud risk in this formular:

Inherent fraud risk – existing controls = residual fraud risk

This means that:

a) Strong/ effective existing controls leave low levels of residual fraud risk,

b) Weak/ ineffective existing control activities leave higher levels of residual fraud risks, and

c) Ineffectiveness in existing controls is a result of weaknesses in those controls.

The team should therefore rate the amount of residual using the established criteria of impact and likelihood (see Section 3.3.3).

The fraud risk assessment exercise should be able to compare the residual risk with the PSE's tolerance levels and risk appetite as set out in the PSE's Risk Management Framework.

3.3.8 Proposed Improvement on Existing Controls to Lower the Residual Fraud Risks

Each residual fraud risks must be compared with tolerance levels set out in the PSE Risk Management Framework based on the following premises:

a) The comparison should be immediately after rating the individual residual fraud risk in the appropriate place in the Risk Identification and Analysis Sheet;

b) The team should propose/ developing controls or actions that eliminate weaknesses in existing control with aim of lowering residual risk to an acceptable level; and

c) The rating is as given in Basing on levels in Table 4 under Section 3.3.3, the Team will propose improvement on mitigations, with a specific focus on addressing the weaknesses identified against each control activity.

Table 5 Shows the decisions on whether or not to propose new mitigation will to be made.

Table 5: Fraud Risk Rating Categories and Decisions on Proposing Mitigations to be Taken

Risk Rate (Impact x Likelihood)	Meaning and Decision
15-25 Extreme Fraud Risk	Very serious concern; highest priority. Proposed mitigations to remedy weaknesses in existing control PSE must take immediate action to implement the proposed controls and review regularly.
10-14 High Fraud Risk	Serious concern; higher priority. Team must propose mitigations to remedy weaknesses in existing controls. PSE must take immediate action to implement the proposed controls and review at least three times a year.
5-9 Moderate Fraud Risk	Moderate concern: steady improvement needed. Team must propose some mitigation to improve the weaknesses. PSE may choose to implement the proposed mitigations after a cost-benefit analysis. Possibly review biannually.
1-4 Low Fraud Risk	Low concern; occasional monitoring. Tolerate/ Accept. Existing controls are deemed affective with minor or nor weaknesses. PSE shall continue with existing measures and but review annually.

Decisions on how to propose controls activities should focusing on conformance of principle 3 of fraud risk management, which requires PSEs to select, develop, and deploy both preventive and detective fraud control activities (See Section 3.4 and Section 3.5).

At the managerial level, and before planning for implementation, a cost-benefit analysis must be performed on the each of the proposed mitigations.

3.3.9 Prepare a Fraud Risk Register

The end result or output of the fraud risk assessment process is duly completed Fraud Risk Register (see Template 5). A Fraud risk register acts as the main repository of fraud risks in all areas of the PSE.

The main section of the fraud risk register is the summary of fraud risks which is prepared in a spreadsheet as given in Template 5.

Other important items that can be added as informative sections of the fraud risk register include:

a) An introduction section where the background information to the PSE, scope and rationale for the register may be given.

b) Methodology section with brief explanation of the approach, criteria and ratings used in fraud risk assessment.

c) Overall profile of fraud risks where a fraud heatmap may be plotted to give a pictorial view of where each fraud risk falls in the heatmap.

d) A summary of all risks in a spreadsheet as exhibited by Template 5, which is arranged following key areas/ processes/ or systems.

e) Detailed fraud risk identification and analysis sheet as attachments to the spreadsheet and arranged in accordance with the to the areas/ processes/ or systems appearing in the spreadsheet.

The above contents are minimum, each PSE, depending on its requirements may need more sections or more information to be included in the Fraud Risk Register.

The Fraud Risk Register should be tabled in various meetings of internal stakeholders, especially the Management Teams, Audit Committee and get approval.

3.3.10 Prepare a Fraud Risk Mitigation Implementation Action Plan

After the finalization of the Fraud Risk Register, each principal risk owner appearing in the register must prepare an action plan.

The purpose of preparing the fraud risk mitigation action is to arrange for timing of implementation of the proposed risk mitigation.

Template 6 provides an example of a Fraud Risk Mitigation Action Plan, which provides the following additional aspects:

a) the proposed implementation dates/ timelines which concretizes the commitment to mitigate the residual fraud risk;

b) the setting of Key Performance Indicators (KPI) or Key Control Indicators (KCI) that will be used as evidence of implementation;

c) the assigning of implementation responsibility for each proposed mitigation; and

d) allocation of resources for funding the implementation, which provides assurance of implementation and links the fraud risk management with the PSE budgeting process.

As with the template for fraud risk register, the mitigation implementation action plan can be customized by adding other columns to fit the specific needs of the PSE. Some prefer to add a column to indicate the cost-benefit decisions for each proposed mitigation.

3.4 Promote Fraud Deterrence and Preventive Measures

The fraud deterrence includes the actions involves in eliminating factors that may cause fraud.

Prevention and deterrence are interrelated concepts. If effective preventive controls are in place, working, and well-known to potential fraud perpetrators, they serve as strong deterrent to those who might otherwise be tempted to commit fraud. Fear of getting caught is always a strong deterrent. Effective preventive controls are, therefore, strong deterrence controls.

Principle 3: Fraud control activities

The PSE 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.

COSO/ACFE (2016)

Fraud prevention involves having arrangements in place that reduce the risk of fraud occurring. Fraud prevention strategies are the first line of defense, and they provide the most cost-effective method of controlling fraud within the PSEs.

It is essential that appropriate preventive and detective techniques are in place. Although fraud prevention and detection are related concepts, they are not the same. While prevention encompasses policies, procedures, training, and communication, detection involves activities and programs designed to identify fraud or misconduct that is occurring or has occurred. Although preventive measure cannot ensure that fraud will not be committed, they are first line of defense in minimizing fraud risk.

One key to prevention is making personnel throughout the PSE aware of the fraud risk management program, including the types of fraud and misconduct that may occur.

They involve a number of factors and/or actors which include an ethical organizational culture, a strong awareness of fraud among employees, suppliers and clients and an effective internal control framework.

3.4.1 Have a Strong and Committed Senior Management Team

The good example set by Senior Management through behavior and actions has very strong influence on the ethical environment of the PSE (i.e., tone at the top).

If senior management is unconcerned about ethical behavior, employees are more likely to commit fraud because they feel that good ethical conduct is not important to the PSE.

Thus, PSE senior management should ensure the following:

a) Setting a good example for all to follow;

b) Making it clear, through statements and policies, that any kind of unethical behavior, especially fraud, will not be tolerated, and

c) Taking actions when cases of misconduct and/or frauds are discovered or reported.

Leadership and fraud deterrence:

Lack of leadership in fraud prevention, detection and response can reduce the likelihood of fraud being reported to management. If staff perceive that controls to respond to fraud are not robust or supported by management, they are much less inclined to report their observations or suspicious.

3.4.2 Operationalize an Ethical Organizational Culture

An ethical organizational culture is one which focuses on and promotes ethical behavior, good administrative practices, and sound controls. The following are the features to be developed:

i. Code of conduct,
ii. Conflict of interest policy,
iii. Employment and service provider screening to ensure prudent employee and third-party due diligence,
iv. Regular ethics and fraud awareness training,
v. Fraud-related controls for activities with a high fraud risk exposure,
vi. System controls to ensure accurate and up-to-date data, and
vii. Communication about investigation outcomes to demonstrate that allegations and incidences of fraud are serious and appropriately dealt with.

These features should be documented and communicated to the entire PSE. Each of these features is explained below:

i. Develop a Code of Conduct

A robust code of conduct and ethics is part and parcel of promoting an ethical culture within the PSE.

PSEs should develop their own code of conduct and ethics in line with the prescribed ethics issued by the President's Office – Public Service Management (PO-PSM).

PSEs should further ensure that all staff are made aware and adhere to the code of conduct and ethics.

Template 7 gives an illustration of a Code of Conduct.

ii. Develop a Conflicts of Interest Policy

Conflicts of Interest should be properly managed within the PSE i.e., conflict between private and public interests.

For instance, restricting private firms (owned by members of management of the PSE) to transact with the same PSE. For that case, PSEs should have in place their own conflict of interest policy.

Template 8 provides specimen a conflict-of-interest policy to be applied within the PSE.

iii. Formulate Whistleblowing Mechanisms

The Whistleblower and Witness Protection Act (2015), defines "whistleblowing: as the act of "making a public interest disclosure", whereby a person makes a disclosure of information in respect of organized crime, corruption offences, abuse of office, unethical conduct, illegal and dangerous activities.

In relation to fraud prevention, a PSE should formulate a whistleblowing policy or reporting mechanism that:

a) Is in in line with the legal stipulations, especially the Whistleblower and Witness Protection Act (2015);

b) Guarantee of confidentiality is a leading inhibitor for people to blow the whistle; and

c) Prevents possible retaliatory acts, by guaranteeing protection

It is therefore recommended that the proposed whistleblowing mechanism should include reporting procedures that will give reporting persons right to choose anonymity when reporting. Template 9 provides sample of a whistleblowing policy.

iv. Conduct Regular Ethics and Fraud Awareness Training

Provision of training is very important so as to create awareness, sensitize and build basic capacity for fraud risk management amongst PSE's staff i.e., create awareness and risk-aware/ ethical culture. Employees play a significant role in fraud prevention and detection.

a) Training needs to be provided to board/council members, Head of Division/Unit, managers, staff, and other close stakeholders. The PSE should ensure that all staff

members should have general awareness of fraud, how they should respond, where to report, some "red flags" of fraud etc.

b) Head of Division/Unit and staff need to be encouraged to comment on fraud risk management procedures that the PSE is adopting, so that they may be improved further as part of the learning culture within the PSE.

c) It is important to carry out the training awareness program along with other policies such as code of conduct.

d) The awareness program can take various forms such as:

- ❖ Training during workers council meetings
- ❖ Printing fraud awareness articles in staff newsletters
- ❖ Use of intranet sites, PSE websites
- ❖ Use of guest speakers to deliver presentation to staff
- ❖ Publishing an abridged version of the entity's fraud control plan
- ❖ Publishing information on fraud prosecutions and outcomes
- ❖ Establishing a fraud control officer network
- ❖ Including fraud matters in the Accounting Officer's weekly communication etc.

v. Screen all New Employees

Employee screening process needs to be undertaken to all persons joining the PSE. This ensures recruitment of staff with at minimum good character, behavior, and qualification. Some practical steps to be taken in the screening of a new staff member include:

a) Verification of qualification through independent source of examination bodies, schools, universities;

b) Policy criminal history search;

c) Reference checks with the two most recent employers; and

d) Consideration through interview and any necessary follow-up of any employment history gaps and reasons for those gaps.

vi. Screen Service Providers

The PSE should carry out a screening process for all types of service providers it wishes to trade with to ensure their identity and reputation.

Normally these are performed through observing the requirements of the Public Procurement Act, CAP 410 and its related regulations when engaging contractors and suppliers to perform works, provide goods, services, and non-consultancy services.

vii. Set Fraud Control of Higher Risk Processes and Activities

Some processes and activities are inherently subject to higher risk of fraud. Thus, they need controls which are actively monitored on regular basis.

Examples of higher inherent fraud risk processes include e.g., cash handling, payroll, procurement, accounts payable, prepayment, travel and subsistence payment, vehicle maintenance, works contracts, grants programs.

Some examples of specific preventive fraud controls that can be applied include:

a) Segregation of duties;

b) Effective procedural controls and management oversight where appropriate;

c) Physical security measures including the use of safe and physical access restrictions;

d) Random and regular quality assurance checks by management; and

e) Hard coded IT System controls (that is access restrictions or monetary value limits for processing.

viii. Control the Risk of Corruption

Corruption is operationally defined as the misuse of entrusted power for private gain. A common form of corruption is aiding and abetting.

a) A thorough risk assessment will consider risk that someone may be engaging in any type of corruption that may be applicable to organization;

b) The PSE should have strategies in place to control the risk of corruption e.g., strong anti- corruption, anti-bribery provisions; vendor audits of high-risk providers; multiple open channels of communication with employees, customers, vendors and other third parties to encourage them report any signs of corruption; and

c) One of the key corruptions is personnel within or outside the PSE can obtain employee or customer data and use such information to obtain credit or for other fraudulent purposes.

3.5 Set Appropriate Fraud Detection Measures

PSE's effective detective controls in place and visible is one of the strongest deterrents to fraudulent behavior. Although detective controls may provide evidence that fraud is occurring or has occurred, they are not intended to prevent fraud.

Fraud detection employs procedures that uncover fraud as soon as possible after it has occurred in the event that the PSE's preventing systems fail.

The measures to detect fraud are categorized in two forms; passive, and active detection measures.

3.5.1 Passive Detection Measures

Passive detection measures include controls that do not require the active and ongoing involvement of management. They rather exist as a means by which fraud is detectable within the PSE such as a reporting hotline. The following are main passive fraud risk detection measures:

i. Effective Internal Controls

Implementation of effective internal controls within the PSEs accounts for about 15% in detecting major frauds (ACFE, 2020).

Thus, the first line of defense is for the management of respective PSEs to ensure effective implementation of internal controls.

The separate Guidelines for Internal Control Frameworks in Public Sector issued by the Ministry of Finance and Planning provide guidance for the PSEs on how to go about implementing effective internal control frameworks within their respective places.

Examples of detective internal controls:

a) Continuous audit through data mining and analysis;
b) Regular bank reconciliation of accounts;
c) Independent confirmation of service delivery where suppliers are paid in advance of services;
d) Physical security e.g., security camera;
e) Job rotation/mandatory leave;
f) Comparison between budgeted and actual figures and the follow-up of discrepancies;
g) Quality assurance;
h) Surprise audits;
i) Audit trails and system access logs and the regular review of these;
j) Competent and professional personnel; and
k) Management review.

ii. Mechanisms to Report Fraud Allegations

Allegations made by employees, contractors and members of the public can often lead to the uncovering of fraud. Thus, the PSE should encourage employees, contractors, service

providers and where relevant, members of the public to report their suspicions of fraud as a key tool for fraud detection.

In view of the above, proper guidance should be made to both employees and external parties to report any fraud allegations within the PSE (e.g., guidance on reporting to line managers, reporting to human resources manager, reporting to fraud risk coordinator, reporting to internal audit and anonymous tip – off or hotline facilities).

iii. Tip-Off or Hotline Facilities

A tip – off or hotline facility provides a method whereby employees and other parties can commutate concerns about potential fraud in an anonymous manner. It minimizes the risk of possible threat of retaliation and negative reactions from superiors.

Hints for operationalizing a hotline facility:

a) It is a single point for staff and public members to report information on suspected fraud

b) It has the advantage of being perceived as being independent of management. PSEs may find it beneficial to outsource the hotline service to a third poverty provider.

c) Although mainly telephone –based, can also sometimes receive reports via other channels such as emails or mail. Thus, formal addresses and electronic formats for submission through website or special PSE's email should be provided.

d) It provides access to a trained interviewer, operates 24 hours a day and it is free of charge

e) Matters reported via the hotline are normally treated with confidentiality to the fullest extent possible

f) A PSE can use the data for fraud allegations to analyze trends and address emerging risks.

iv. Whistle blowing and Public Interest Disclosures

Whistle blowing refers to the reporting, in the public interest, of information which amounts to the breach for code of conduct and ethics (including fraud) by public servants.

PSEs should provide information about whistle blowing such as the type of information that attracts whistle blowing protections and the person to whom the disclosure can be made to all staff through various means like during fraud awareness training, provision of leaflets etc.

Above all, PSEs should prepare and operationalize their own whistle blowing policy (see also template 9 for a sample policy).

3.5.2 Active Detection Measures

Active detection measures require the assertive involvement of management. By virtue of their nature, they are designed to detect or assist in detecting fraud within the PSE.

i. Monitoring and Review Activities to Detect Internal Fraud

There are a number of "red flags" or "early warning signs" of fraud activity which can be used to help profile possible internal perpetrators. Table 2 below provides for a few examples. PSEs should thus monitor and review activities on regular basis to detect such "red flags" for possible fraud risks.

Table 6: Signs (Red Flags) for Fraud Risks

Early warning signs: people (individuals)	Early warning signs: areas or functions
Unwillingness to share duties refusal to take leave	Financial information reported is inconsistent with key performance indicators.
Refused to implement controls.	Abnormally high and increasing costs in a specific cost center function.
The replacement of existing suppliers upon appointment to a position or unusually close association with a vendor or customer.	Dubious record keeping
A lifestyle above apparent financial means, the provision of gifts to other staff members.	High overheads
Failure to keep records and provide receipts.	Bank reconciliation not up to date.
Chronic shortage of cash or seeking salary advances.	Inadequate segregation of duties.
Past legal problems (including minor previous thefts)	Reconciliations not performed on a regular basis.

ii. Analysis of Management Accounting Reports

The analysis of management accounting reports can reveal anomalies which may be indicative of fraud.

Monthly actual versus budget comparison reports by departments, reports comparing expenditure against prior periods and reports highlighting unusual trends in bad or doubtful debts all may reveal areas which should be further investigated.

iii. Hot Spot Analysis

Allegations of unethical behavior or frauds raised through the PSE's reporting mechanisms (hotline, reports to management via email and other methods) can be "mapped" to show hot spots of potential fraud throughout the PSE.

This can further be used to target the activities of internal audit, an investigation team or the fraud risk coordinator.

iv. Data Mining- Post Transactional Review

Data mining refers to the application of analysis techniques to the PSE's financial and operational data which helps to detect some indicators of fraud, misconduct, and errors.

There are two types of data mining /analysis, namely:

i. *Retrospective review* – refers to extraction of historical data (usually data relating to more than one year) using data analysis software.

ii. *Continuous Auditing / Continuous Monitoring* (CA/CM) – refers to the collection and analysis of current data on a real or near real- time basis i.e daily, weekly and/or monthly. CA is generally considered to provide the internal auditor with information regarding risk and controls while CM is generally considered to be a management monitoring function.

Data mining can uncover the following:

a) Analysis of suspicious transactions e.g., duplicate payments or climes;

b) Identification of unusual relationships e.g., employee bank account matches vender bank account;

c) Assessing the effectiveness of internal controls e.g., password sharing, employees remaining on the payroll after terminations/resignation etc.; and

d) Identification of irregular trends over periods e.g., supplier favoritism.

An ability to analyze large volumes of transactions over periods of time rather than relying on sampling techniques.

v. Monitoring and Review Activities to Detect External Fraud

All PSEs that collect revenue or administer government payments should conduct reviews across the various revenue and payment types. The reconciliation of control numbers is imperative to rest assure financial objectives

Based on previous experience, knowledge of their customers, and evidence from within their systems or from outside information, PSEs may undertake reviews that examine a recipient's circumstances where there is a perceived risk of fraud.

The aim of such reviews is to detect a deliberate error, omission, misrepresentation, or fraud on the part of a customer.

Review activity should be targeted to areas of higher risk, and the PSE should pursue the most productive method for undertaking reviews.

Data mining / matching discussed earlier on is a cost-effective method of supporting reviews, including cross-PSEs approaches.

vi. Detecting Fraud by External Service Providers

External fraud includes the fraudulent conduct of service providers who charge the PSEs for goods or services that are not delivered or delivered in an incomplete way. Most cases of external service provider fraud are discovered through day-to-day contract management and associated controls.

The aim of contract management is to ensure that deliverables are provided to the required standard, within the agreed timeframe, and achieve value for money. A central risk to the success of a contract is the management of external service provider performance, including the potential for fraud, or inappropriate conduct by the external service providers.

In view of the above, PSEs should observe the requirements of the Public Procurement Act, CAP 410 and its related Regulations on issues relating to contract management.

vii. Partnering with Other Institutions

The sharing of information about risk factors and fraud perpetrators within the PSEs and across the public sector is important in the prevention and detection of fraudulent activity.

Liaison with other institutions may also help target detection activities and the sharing of better practices.

Any forum which brings together organizations with a similar business profile can be used as an opportunity to discuss fraud risk, prevention, detection, and response

viii. Utilizing the Role of Internal Audit

Responsibility for managing the risk of fraud, like responsibility for managing all risks, rests with management as part of its ongoing responsibilities.

However, internal audit can assist a PSE to manage fraud by advising on the risk of fraud and the design or adequacy on internal controls. It can also assist in detecting fraud by considering fraud risks as part of its internal audit planning and being alert to indicators that fraud may have occurred.

Audit teams may discover instances of fraudulent activity in the course of conducting internal audits. Internationally, internal audit has been responsible for detecting 15% of all frauds identified in the government sector (ACFE, 2020). PSEs should for that purpose ensure strengthened internal audit units in terms of adequate skilled and competent internal audit staff, financial and other material resources.

3.5.3 *Continuous Monitoring of Fraud Detection*

The PSE should develop ongoing monitoring and measurements to evaluate, remedy and continuously improve the PSE's fraud detection techniques.

If deficiencies are found, management should ensure that improvements and corrections are made as soon as possible. Management should institute a follow up plan to verify that corrective or remedial actions have been taken.

The PSE should establish measurement criteria to monitor and improve fraud detection. Measurable criteria include:

a) Number of known fraud schemes committed against the PSE;
b) Number of statuses of fraud allegations received by the PSE that required investigation;
c) Number of fraud investigations resolved;
d) Number of employees who have/have not signed the ethics statements;
e) Number of employees who have/have not completed ethics training sponsored by the organization;
f) Number of whistleblower allegations received via the organization's hotline;
g) Number of allegations that have been raised by other means;
h) Number of messages supporting ethical behavior delivered to employees by executives;
i) Number of service providers who have/have not signed PSE's ethical behavior requirements;
j) Number of customers who have signed the organization's ethical behavior requirements; and
k) Number of fraud audits performed by internal auditors.

3.6 Establish Appropriate Fraud Response Procedures

Fraud response refers to a plan of action put in place when a suspected fraud is discovered or reported.

The purpose of this plan is to define the responsibilities for action, such as:

a) Investigating fraud incidents and taking appropriate action;
b) Securing evidence for disciplinary and/or criminal action;
c) Preventing further loss;
d) Recovering losses;
e) Establishing lines of communication with the police;
f) Reviewing internal controls following a fraud; and
g) Fraud reporting arrangements.

Principle 4: Fraud investigation and corrective action

The PSE 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.

COSO/ACFE (2016)

3.6.1 Actions to be taken When a Fraud is Reported

Once a suspected fraud has been reported or identified, an assessment of the situation should be made. Consideration should be given to the following factors:

a) The source of discovery of the suspected fraud;
b) The authenticity of the information initially received; and
c) Line management's initial assessment of the circumstances involved.

All cases should be treated confidentially and handled carefully to ensure no-one is harmed by false allegations, that anyone committing a fraud is not forewarned, or that anyone reporting a fraud is not victimized.

The purpose of an assessment is to allow a decision to be made on the appropriate action to be taken. This could include:

a) Whether or not a formal internal investigation is required;

b) Whether or not the matter should be reported to the Police;

c) Whether or not the matter requires reporting to another agency such as PCCB;

d) Who should conduct an internal investigation;

e) Whether or not action needs to be taken to secure the organization's assets, resources, or information; and

f) Whether or not a media release is required.

3.6.2 Conducting Formal Internal Investigation

In case it has been determined that fraud exist, the Accounting Officer or Higher Authority within the PSEs will appoint the investigation team.

Investigation may involve people from the organization itself, such as an internal auditors or finance managers, or may involve external parties who have particular qualifications, skills, experience and are engaged specifically to assist the investigation. The decision will depend on the circumstances and the relevant expertise required.

In any event, the person chosen must have the appropriate qualifications and experience to carry out an investigation in respective area. Principal Officers or line managers may be required to assist the investigator but should not become directly involved in the investigation process, nor should managers attempt to unduly influence the investigation report.

3.6.3 Involvement of the Police and PCCB

Suspected fraud should be reported to the Police where there is likelihood that criminal activity has taken place. If the suspected fraudulent activity is considered to be of this nature and the matter is reported to the Police, no attempt must be made by the PSE's personnel to question the employee(s), or third parties involved as this could prejudice future Police investigations and subsequent prosecutions.

If the fraud involves corruption, then it must be reported and dealt with the PCCB. Report from PCCB after investigation will also be furnished to the PSE for taking relevant actions on the matter.

3.6.4 Securing Information and Assets

In some cases, it may be necessary to act to secure assets and preserve information. Such actions could include:

- The appointing authority suspending from work the suspected employee(s), pending the outcome of any investigation.
- Securing the suspect's station and all documentation (hard and electronic documentation) and making inaccessible to the suspect and any other unauthorized employees.

3.6.5 Dealing with the Media

In some cases, particularly where a fraud is of high value, it may be necessary to deal with the media. In such cases the Accounting Officer (assisted by his/her experts i.e., public relations officer, legal officer etc.) is responsible to prepare a media release.

When preparing a media release, it is important to:

a) Keep it short, factual, and straightforward;
b) Not speculate about what might have happened;
c) Be honest about what is not yet known;
d) Make concerns clear;
e) Detail what is being done in response to the situation; and
f) Be very careful about attributing blame.

It is also very important that a single point of contact be established for dealing with the media. The PSE should ensure professionalism and protecting its image. No-one, apart from the designated point of contact, should speak to the media.

3.6.6 Instituting Disciplinary Procedures

A PSE may invoke administrative remedies in addition to any other actions or penalties that may be imposed by law or regulations. Such remedies will differ from case to case but may include fines, demotion, termination or employment, or cancellation of contracts.

Other actions to be taken include recovering fraud losses caused by the fraudulent employee. These include actual losses and all other related administrative costs. Procedures outlined in the relevant laws e.g. Public Finance Act, CAP 348, Public Service Act, CAP 298 and Public Procurement Act CAP 410 should be observed.

Where contractors and suppliers are involved, apart from recovering losses, they should also be blacklisted in working with the PSEs as per Public Procurement Act, CAP 410.

3.6.7 Documenting the Results of an Investigation

Irrespective of whether the investigation is internal or external proper records should be maintained for all investigations.

This includes for the investigation itself, and any consequent proceedings and changes to internal control arrangements. The standard for such record keeping should be in line with best practice for investigation.

3.6.8 Reporting the Results of an Investigation

Once an investigation is concluded the results should be reported to the appropriate bodies of the PSE. Also, an annual fraud report should be presented detailing:

a) All instances of fraud reported against the organization;
b) Th e outcome of internal fraud investigations;
c) The status of cases of fraud referred to external agencies for investigation;
d) The results of any completed prosecutions or administrative actions; and
e) Internal control modification made subsequent to any fraud.

3.6.9 Review of Internal Controls after a Fraud

An important result or outcome of a fraud investigation is identification of the control failures that allowed the fraud to occur.

In each instance where a fraud is detected a review should be undertaken to assess the adequacy of the PSE's internal controls and determine what action needs to be taken.

Where improvements are required, they should be implemented as soon as possible by the relevant head of Division/Department, Unit and/or Accounting Officer depending on the level of authority. Monitoring the implementation and follow-up to ensure that all actions have been completed should be done by relevant organs as per the structure of the PSE.

3.7 Establish Fraud Risk Management Reporting Process

Effective fraud risk reporting contributes to good corporate governance by providing reliable and current information to Boards/Accounting Officer or other Higher Authority, Senior Officials, and other stakeholders (i.e., both internal and external) regarding the fraud risks faced by the PSE as well as the treatment plans in place to manage these fraud risks. The availability of this information can be used to support management decision-making.

3.7.1 Prepare the Fraud Risk Reports

The Fraud Risk Coordinator should be responsible for coordinating and drafting fraud risk reports to ensure consistency in standards and format.

The frequency of fraud risk reporting should reflect the cycle of the PSE's regular internal reporting (i.e., monthly, or quarterly progress reporting). At a minimum, an organization should update and report on its fraud risk profile on an annual basis.

Template 10 provides format of Fraud Risk Management Quarterly Implementation Report.

3.7.2 Format of Fraud Risk Reports

The way that risk information is presented can make a huge difference in the value it adds. Report format is not restrictive, but the information provided depends on its level e.g., strategic level and operational level.

Reporting at the strategic level consists of strategic fraud risks to the PSE on how they are periodically managed. It also includes fraud risk heat maps which are useful as they graphically illustrate the relative severity of fraud risks in relation to each other.

Reporting at the operational level is detailed and the table format is best suited to report on how fraud risks are being managed.

These reports are used by audit committees, fraud risk coordinators and fraud risk owners to monitor and manage the update, implementation, and review of fraud risk management activities/plans.

3.8 Monitor and Evaluate the Fraud Risk Management Framework

Monitoring and Evaluation of a fraud risk management framework provides assurance that the framework remains fit for purpose and is customized to meet changing organizational circumstances and new leading practices.

Principle 5: Fraud risk monitoring activities

The PSE 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.

COSO/ACFE (2016)

3.8.1 Monitoring the Framework

Monitoring of the fraud risk management framework, fraud risk management process and control is an essential facet to enable continuous improvement.

Monitoring refers to continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.

Monitoring generally seeks to address the following:

a) Fraud risks are being effectively identified and appropriately analyzed;
b) There is adequate and appropriate implementation of fraud risk management strategies and controls; and
c) There is effective monitoring and review by management an executive to detect changes in fraud risks and controls.

Monitoring at the PSE level should first be carried out by management. This should normally be done through periodic reporting on the way fraud risk management strategies and controls are being implemented.

The Fraud Risk Coordinator will play a key role in the PSE regarding effective reporting.

The following will help the PSE in ensuring monitoring of fraud risk management activities:

a) Preparation and submission of quarterly fraud risk management implementation reports;

b) Semi-Annual review and updating of the fraud risk register; and

c) Periodic review and updating of the fraud risk management framework as put forth in the fraud risk policy

3.8.2 Evaluation of the Fraud Risk Management Framework

Evaluation of the fraud risk management framework entails periodic collection of information pertaining to the way the framework was implemented. Unlike monitoring, evaluation is time-bound and periodic in nature, it will take place at particular intervals before, during (thereby aiding improvement) or at the end of a project.

Management will be responsible for carrying out evaluation of the framework. Also, other organs like internal audit, external audit, professional bodies, and IAGD will carry out evaluation at different prescribed/ defined intervals.

3.8.3 Continual Improvement of the Fraud Risk Management Framework

The key objective of continual improvement is to ensure the ongoing relevancy and effectiveness of fraud risk management activities within the PSE.

Hence, to achieve the greatest benefits from continuous improvement, it must encompass all fraud risk management framework elements including the process, capability, behaviors, tools and templates and reporting structures, and the practices used to manage actual risks.

The initiatives that are identified during monitoring and review activities should be taken on board, prioritized, and then included within the fraud risk management strategy and plans. They should further be approved and implemented accordingly.

Results of Fraud Investigation should be used to improve fraud risk management processes and procedures.

SECTION IV

4 TEMPLATES

This section provides some illustrations and the key templates for use as minimum disclosure in developing and implementing the fraud risk management framework at a particular PSE.

***Template 1:* Format and Key Contents of the Fraud Risk Policy**Some typical key content of the fraud risk policy includes, among other things:

(i) Introduction

This may outline the meaning and impact of fraud and corruption to the PSE in the context of its operating environment. To remove any doubt, it may beneficial to include a clear statement of the PSE's zero-tolerance stance on fraud and corruption.

(ii) Statement of purpose or objectives

This is a statement of intent and outlines why the policy is being written or why fraud risk management is being adopted in the PSE. It explains the intended outcomes of the policy.

(iii) Policy statements

The key features of the PSE's policy should be summarized as a series of direct, unambiguous statements which highlight the PSE's philosophy, attitudes and commitment towards fraud risk management. These statements should outline what the PSE will do to control fraud and corruption from both internal and external sources.

(iv) Applicability

There should be a concise description of who will be affected by the policy, including both internal and external stakeholders.

It may include a list of officials or organs to whom the policy is relevant or on which it imposes particular requirements. Further, it may outline individual responsibilities, as well as the links between stakeholders.

(v) Definitions

Specific terms or key principles used throughout the policy should be defined. This will clarify meaning and avoid any ambiguity when the policy is applied.

(vi) Fraud Risk Management Governance Structure

The policy should outline responsibilities and accountabilities of various officials and organs with respect to fraud risk management.

(vii) Fraud Risk Management Principles and Procedures

a) The standard and procedures adopted by the policy in managing fraud risks should be outlined. The principles/ procedures should be in line with any] of the internationally adopted standard i.e., COSO, or ISO 31000 etc.

Some key procedures that may be included in the policy are:

b) Risk assessment process Internal controls

c) Internal reporting External reporting

d) Public interest disclosures Investigations

e) Code of conduct

f) Staff education and awareness

g) Client and community awareness.

(viii) Reference or authority

This lists the relevant legislation, or government directives or standards under which the PSE operates and which are relevant to the policy.

(ix) Administrative details

The policy should provide for the names of the approving authority (i.e.) i.e. name and signature of the Chairman of the Board/Council; name and signature of the Accounting Officer and date of approval.

Suggested date for review may also be included.

(x) Annexes

All relevant fraud risk management templates (samples of key documents/forms/and sheets) should be appended to the policy.

Template 2: Fraud Risk Management Framework

1. EXECUTIVE SUMMARY

i. Definition of fraud
ii. Statement of attitude to fraud
iii. Code of conduct (relationship to)
iv. Relationship with entity's other plans
v. Roles and accountabilities

2. SUMMARY OF FRAUD CONTROL STRATEGIES

i. Appointment of fraud control officer
ii. External assistance to the fraud control officer
iii. Fraud control responsibilities
iv. Fraud risk management (including fraud risk assessment)
v. Fraud awareness
vi. Fraud detection
vii. Fraud reporting
viii. Investigation of fraud and other improper conduct
ix. Internal control review following discovery of fraud
x. Fidelity guarantee and criminal conduct insurance
xi. Internal audit program

3. FRAUD RISK MANAGEMENT

i. Regular program for fraud risk assessment
ii. Ongoing review of fraud control strategies
iii. Fraud risk assessment
iv. Implementation of proposed actions

4. PROCEDURES FOR REPORTING FRAUD

i. Internal reporting
ii. Reports by members of staff
iii. Protection of employees reporting suspected fraud
iv. External anonymous reporting
v. Reports to the police
vi. Reports to external parties
vii. Administrative remedies
viii. Recovery of the proceeds of fraudulent conduct
ix. Reporting requirements

5. EMPLOYMENT CONDITIONS

i. Pre-employment screening
ii. Annual leave

6**. CONFLICT OF INTEREST**

i. The impact of conflicts of interest
ii. Register of interests
iii. Conflict of interest policy (*See Template 8*)

7**. PROCEDURES FOR FRAUD INVESTIGATION**

i. Internal investigations
ii. External investigative resources
iii. Documentation of the results of the investigation

8**. INTERNAL AUDIT STRATEGY**

i. Internal audit capability
ii. Internal audit fraud control function

9. REVIEW OF FRAUD CONTROL ARRANGEMENTS

NB: The Fraud Risk Management Framework will normally include the Price Risk Management Policy as part of the Framework document. Therefore, the contents under template 1 will adopted for the purpose.

Template 3: Common Fraud Categories and Scenario

Note: the list does not represent a complete list of common types of fraud exposures, nor will all of these types be applicable to all organizations.

ASSETS MISAPPROPRIATION
Including: Cash, Non-Cash

Cash

Theft of cash

- Stealing from petty cash.
- Taking money from the safe boxes.
- Skimming of cash before recording revenues or receivables (understanding sales or receivables).
- Stealing incoming cash or cheques through an account set up to look like a bona fide payee.

False payment requests

- Employee creating false payment instruction with forged signatures and submitting it for processing. False email payment request together with hard copy printout with forged approval signature.
- Taking advantage of the lack of time which typically occurs during book closing to get false invoices approved and paid.

Cheque fraud

- Theft of company cheques.
- Duplicating or counterfeiting of company cheques.
- Tampering with company cheques into a third-party account without authority.
- Cheque kiting (a fraud scheme using two deposit accounts to withdraw money illegally from the bank). Paying a cheque to the company knowing that insufficient funds are in the account to cover it.

Billing schemes

- Over-billing customers.
- Recording of false credits, rebates or refunds to customers.
- Pay and return schemes (where an employee creates an overpayment to a supplier and pockets the subsequent refund).
- Using fictitious suppliers or shell companies for false billing.

Misuse of accounts

- Wire transfer fraud (fraudulent transfers into bank accounts). Unrecorded sales receivables.
- Employee account fraud (where an employee is also a customer and the employee makes unauthorized adjustments to their accounts).
- Writing false credit note to customers with details of an employee's personal bank account or of an account of a company controlled by the employee.
- Stealing passwords to payment systems and inputting series of payments to own account.

Non-Cash

Inventory and fixed assets

Theft of inventory.

- False write offs and other debits to inventory. False sales of inventory.
- Theft of fixed assets, including computers and other IT related assets.
- Theft or abuse of proprietary or confidential information (customer information, intellectual property,
- pricing schedules, business plans, etc).
- Receiving free or below market value goods and services from suppliers. Unauthorized private use of company property.
- Employees trading for their own account.

Procurement

- Altering legitimate purchase orders.
- Falsifying documents to obtain authorization for payment. Forging signatures on payment authorizations.
- Submitting for payment false invoices from fictitious or actual suppliers. Sending fictitious or duplicate invoices to suppliers.
- Improper use of company credit cards.
- Marked up invoices from contracts awarded to supplier associated with an employee. Sale of critical bid information, contract details or other sensitive information.

Payroll

- Fictitious (or ghost) employees on the payroll.
- Falsifying work hours to achieve fraudulent overtime payments. Abuse of commission schemes.
- Improper changes in salary levels.

- Abuse of holiday leave or time off entitlements. Submitting, inflated or false expense claims.
- Adding private expenses to legitimate expense claims. Applying for multiple reimbursements of the same expenses. False workers' compensation claims.
- Theft of employee contributions to benefits plans.

Financial

- Improper revenue recognition
- Holding the books open after the end of the accounting period. Inflation of sales figures which are credited out after the year end. Backdating agreements.
- Recording fictitious sales and shipping. Improper classification of revenue.
- Inappropriate estimates for returns, price adjustments and other concessions. Manipulation of rebates.
- Recognizing revenue on disputed claims against customers. Improper recording of consignment or contingency sales.
- Over/under estimating percentage of work completed on long-term contracts. Incorrect inclusion of related party receivables.
- Side letter agreements (agreements made outside of formal contracts).
- Round tripping (practice whereby two companies buy and sell the same amount of a commodity at the same price time. The trading lacks economic substance and results in overstated revenues).
- Bill and hold transactions (where the seller bills the customer for goods but does not ship the product until a later date).
- Early delivery of product/services (eg. partial shipments, soft sales, contracts with multiple deliverables, up front fees).

IT Related Fraud

- Spoofing – act of forging a machine's identity or using other techniques to attempt illegal access to IT system.
- Key person dependency – relying on one person to maintain PSE's network, computer facilities which compromise day to day activities when that person is absent.
- Data exposure – someone might have unauthorized access to PSE's sensitive data.
- Natural disaster – e.g. lighting, floods etc could cause serious problems on IT operations.
- Software defect – unintentional defects in software received from vendors.
- Denial of service – An attack intended to consume some resources to provide service (e.g., disk space, network bandwidth, CPU capacity etc.).
- Malware – malicious code, which is software designed to disrupt services i.e., virus, Trojan, worms, back doors.

- Misappropriation – use of IT resources for unauthorized activities.
- Former employees – intentional actions by form employees using knowledge gained while an employee.
- Breach of physical security to IT equipment and facilities etc.
- Online criminals' use of programs that help them automatically generate attacks based on publicly available information about vulnerabilities
- Unauthorized program modification schemes. This category of computer - generated insider schemes typically involve making unauthorized changes to automated payment or accounting software programs such as Processing undocumented transaction codes, Balance manipulation, Lapping schemes, Fraudulent file modifications
- File alteration and substitution schemes such as Accessing a live master file, Substitution of a dummy version of a real file.

Template 4: Template 10: Fraud Risk Assessment Sheet

Template 10: Fraud Risk Assessment Sheet

Process/System being Assessed	*Write the Process impacted by the Fraud risk*						
Fraud Risk Title	*Provide a brief title of the risk*			**Fraud Risk ID**	*Define the identity of the risk*		
Fraud Risk Description	*Provide a brief description of the Fraud risk*						
Principal Fraud risk ownerr	*Include the title of the person managing the Fraud risk and the area where the Fraud risk falls*						
Supporting owner(s)	*Provide the title of other persons affected by the Fraud risk*						
Fraud Risk Category	*Is it a Corruption, Asset Mis appropriation of Fraudulent Financial report.*						

Fraud Risk Causes and Consequences			
Causes *(Provide a list of sources or causes that may lead to risk materializing e.g., events, decisions, actions, and processes)*		**Consequences** *(Provide a description of what will happen if the risk materializes)*	
1.		1.	
2.		2.	
3. etc.		3.etc.	

Inherent Fraud risk analysis *(Tick the impact and likelihood of Fraud risk assuming the current controls do not exist or completely fails)*

Inherent risk	**Impact (I):**	4	VERY HIGH	HIGH	MODERATE	LOW	VERY LOW
	Likelihood (L):	3	VERY HIGH	HIGH	MODERATE	LOW	VERY LOW
Risk rating	**I x L:**			**12**	**HIGH**		

Key Fraud risk mitigation/controls currently in place: *(List mitigations in place, rate and colour effectiveness and document separately weakness if control is rated below effective)*

No.1	*Mitigation/Control (Write in the summary of the existing control)*	Effectiveness of preventive controls *(Indicate appropriate color, effective, partially effective, or ineffective)*	Rating	Effectiveness of corrective controls *(Indicate appropriate color, effective, partially effective, or ineffective)*	Rating
1.		Partially - Effective		Partially -Effective	
2.		Effective		Ineffective	
3.		Ineffective		Ineffective	
		Average Preventive		**Average Corrective**	

Residual Fraud risk analysis *(tick the impact and likelihood of the Fraud risk that remains after considering how the current mitigation have reduced the inherent risks based on corrective or preventive control)*

Residual Fraud	**Impact:**	4	VERY HIGH	HIGH	MODERATE	LOW	VERY

risk							LOW
	Likelihood:	2	VERY HIGH	HIGH	MODERATE	LOW	VERY LOW
Risk rating	**I X L:**	**8**	**MODERATE**				

Proposed Mitigating/ Control to be taken: *(List mitigations/controls that must be taken to mitigate the residual Fraud risk base your proposal on: Unmitigated cause to the risk or identified weakness in current control)*

No.	**Proposed control**	**Key Control Indicator (KCI)**	**Resources Required**
1.			
2.			
3. etc.			

Template 5: Extract of a Fraud Risk Register

Name of Area/Process/ System (Process/System being Assessed)	**FRAUD RISK TITLE** (As it appears in the identification sheet)	**CATEGORY OF FRAUD RISK** (As described in the identification sheet)	**FRAUD RISK ID** (As in the identification sheet)	**RESIDUAL FRAUD RISK ASSESSMENT** (As in the identification sheet)		**FRAUD RISK RATING** (I X L) [Product (in number) of multiplying Impact by Likelihood]	**FRAUD RISK STATUS** (Write either EXTREME, HIGH, MEDIUM or LOW and shade it with the appropriate color)	**PRINCIPAL FRAUD RISK OWNER** (As in the identification sheet)	**PAGE** (Write the page number to make reference to the attached identification sheet)
				IMPACT (I)	**LIKELIHOOD (L)**				
Procurement	Fraud Risk. P-FR.01								
	Fraud Risk. P-FR.02								
	Fraud Risk. P-FR.03								
	Etc.								
	Etc.								
Finance	Fraud Risk. F-FR.01								
	Fraud Risk. F-FR.02								
	Etc.								
	Etc.								

i. Information in the fraud risk register is summaries of what is appearing in the fraud risk identification and analysis sheet.

ii. At the end of the fraud risk register attach the fraud risk identification and analysis sheets in serially according to the list of the fraud risks in the register, provide page numbers on each fraud risk identification and analysis sheet so that the page number will be filled-in in the last column of the fraud risk register. This will facilitate quick referencing from fraud risk register to identification sheets.

Template 6: Extract of Fraud Risk Treatment Action Plan

Department/Unit: .....
Date of review: ..... Compiled by: ..... Date: .....
Reviewed by: ..... Date: .....

Fraud Risk title & ID (From Fraud Risk Register in priority order)	**Area/ Process/ System Affected** (As appearing in the Fraud Risk Register)	**Proposed Treatment/Control Options** (From Fraud Risk Register)	**Person Responsible for Implementation of Treatment Options** (As mentioned in the Fraud Risk Register)	**Timetable for Implementation** (Give specific start and end dates for implementing the mitigation)	**Key Performance Indicator (KPI) or Key Control Indicator (KCI)** (How will this fraud risk and treatment options be monitored or evidenced of implementation)	**Estimated Costs** (Budget)

Template 7: Code of Conduct

(PSEs should adopt the Public Service Code of Conduct issued under Public Service Act CAP 298).

Employees are required to always adhere to the Code of Conduct when performing their duties and representing the PSE. The Code of Conduct requires employees to:	
1	Comply with the condition of employment
2	Act with honesty and integrity
3	Demonstrate respect to other people
4	Avoid actual and perceived conflicts of interest, including any personal activities or financial interests which may conflict with their commitment to effectively perform their job
5	Maintain confidentiality of information gained from employment with the PSE and avoid disclosure of this information outside the normal requirements of their job
6	Refuse gifts from clients and suppliers, or from people or PSEs in any way connected with clients or suppliers
7	Avoid any form of racial discrimination or abuse
8	Seek prior approval for personal use of any PSE equipment, with all personal use to be officially registered
9	Agree to the PSE's approved conditions for use of telephones, IT systems and the internet
10	Only make media comment concerning the PSE if requested to do so by the Accounting Officer

ACKNOWLEDGEMENT I acknowledge I have received, read, and will comply with the Code of Conduct
Employee Signature: **Date:**
Employee Name:

Template 8: Conflict-of-Interest Policy for PSE

PURPOSE

This policy complements the Organization's Code of Conduct by establishing a framework for identifying and resolving conflicts of interest.

DEFINITION OF CONFLICT OF INTEREST

A conflict of interest is a situation in which an employee's private interests, including associations or relationships, can or can appear to influence the performance of their official duties.

PSE POLICY

Employees are expected to avoid or effectively resolve any actual or perceived conflict of interest situations in which private interests could influence their ability to effectively perform their duties.

Employees must not, directly, or indirectly:

- Place themselves in a situation, in any official matter, where private interests could lead to questions about how objective their actions or decisions are in the matter,
- Undertake outside employment, or other private arrangements that are, or may appear to be, in conflict with the performance of their duties,
- Seek or receive a benefit by giving preferential treatment to any person while performing their duties,
- Seek or accept a benefit from information acquired during the course of their duties,
- Use the PSE's property to serve their private interests, unless authorized to do so, or
- Solicit or accept gifts or other benefits that are connected directly or indirectly with the performance of their duties.

SCOPE OF POLICY

This policy applies to:

- Employees of the PSE, and
- Those under contract to the PSE for the provision of professional services.

RESPONSIBILITIES

- Responsibility for the disclosure of conflict-of-interest situations rests with the employee. This ongoing obligation begins, but does not end, when an employee is first employed and is required to disclose any conflicts.

- Managers/Supervisors of employees who have disclosed a conflict of interest are required to state how that conflict will be avoided or managed
- The Head of Human Resources will ensure that all new employees sign a conflict-of-interest disclosure form.
- The Head of Human Resources will maintain the PSE's Conflict of Interest Register.

DISCLOSURE OF INTEREST

Disclosure is a confidential procedure that is designed to protect both the employee and the PSE from unfair allegations of conflict of interest. The disclosure of interest can be made at any of the following two stages:

- At the commencement of work with the PSE, all new employees will be required to read the Conflict-of-Interest Policy and disclose any private interests (such as business, financial or other personal interests), they have or might be seen to affect the performance of their official duties.

- During their employment with the PSE, employees are required to disclose any changes in their circumstances that would alter their previously disclosure statement. This includes the acceptance of any gifts or benefits.

CONFLICT OF INTEREST REGISTER

- Disclosure statements for all the PSE's employees will be kept by the Head of Human Resources.
- All disclosures will be treated as strictly confidential and access to information in the Conflict-of-Interest Register will be limited to those with an authorized need to know.

Template 9: Whistle Blowing Policy

INTRODUCTION

This whistleblowing policy has been introduced to enables employees to raise concerns about what is happening at work, particularly where those concerns relate to unlawful conduct, financial malpractice or dangers to the public or the concerns are raised and dealt with at an early stage and in an appropriate manner. It is in line with {cite the relevant Act}

The PSE is committed to its whistleblowing policy. If an employee raises genuine concern under this policy, he or she will not be at risk of losing their job, nor will they suffer any form of detriment as a result. As long as the employee is acting in good faith and in accordance with this policy, it does not matter if they are mistaken.

How the whistleblowing policy differs from the grievance procedure

This policy does not apply to raising grievance about an employee's personal situation. These types of concern are covered by the PSE's grievance procedure. The whistleblowing policy is primarily concerned with where the interests of others or of this PSE itself are at risk. It may be difficult to decide whether a particular concern should be raised under the whistleblowing policy or under the grievance procedure or under both. If an employee has any doubt as to the correct route to follow, this PSE encourages the concern to be raised under this policy and will decide how the concern should be dealt with.

Protecting the employee

This PSE will not tolerate harassment or victimization of anyone raising a genuine concern under the whistleblowing policy. If an employee requests that their identity be protected, all possible steps will be taken to prevent the employee's identity becoming known. If the situation arises where it is not possible to resolve the concern without revealing the employee's identify (e.g. if the employee's evidence is needed in court), the best way to proceed with the matter will be discussed with the employee. Employees should be aware that by reporting matters anonymously, it will be more difficult for the PSE to investigate them, to protect the employee and to give the employee feedback.

The procedures for protecting the employee or whistleblowers should follow the procedures established under section 9 -11 of Whistleblower and Witness Protection Act, 2015.
Accordingly, while the PSE will consider anonymous reports, this policy does not cover matters raised anonymously.

How to raise a concern internally

Step 1

If an employee has a concern about malpractice, he or she should consider raising it initially with their

line manager. This may be done orally or in writing. An employee should specify from the outset if they wish the matter to be treated in confidence so that appropriate arrangements can be made.

Alternatively, employees can call the 24-hour whistleblowing telephone hotline. This service is strictly confidential, and callers will not be asked to give their name if they do not want to.

Step 2

If these channels have been followed and the employee still has concerns, or an employee feels that they are unable to raise a particular matter with their line manager, for whatever reason, they should raise the matter with their head of department, the head of human resources or the chief internal auditor.

Independent advice

If an employee is unsure whether to use this procedure or wants independent advice at any stage, they may contact …….. at work or call through telephone No: their lawyers can give free confidential
advice at any stage about how to raise a concern about serious malpractice at work. An employee can, of course, also seek advice from a lawyer of their own choice at their own expense.

How the matter will be handled

Once an employee has informed the PSE of his or her concern, the concerns will be examined and the PSE will assess what action should be taken. This may involve an internal enquiry or a more formal investigation. The employee will be told who is handling the matter, how they can contact him/her and whether any further assistance may be needed. If the employee has any personal interest in the matter, this should be declared by the employee at the outset. If the employee's concern falls more properly within the grievance procedure, then they will be advised of this.

External contacts

It is intended that this policy should give employees the reassurance they need to raise concern internally. However, this PSE recognizes that there may be circumstances where employees should properly report matters to outside bodies, such as regulators or the police. It is advised for the employee to contact…. for the procedures to follow

Matters raised maliciously
Employees who are found maliciously raise a matter that they know to be untrue will be subject to the disciplinary policy.

Template 10: Format of a Fraud Risk Management Quarterly Report

1.0 Introduction

Provide the brief introduction of the Entity and key Fraud Risk within the entity

2.0 Overview of Fraud Risk Identified Its Mitigation Plan

Provide the overview of the fraud risk Identified and the mitigations in place to mitigate those fraud risk

3.0 Achievements during implementation of the proposed mitigations
4.0 Challenges encountered during implementation of proposed Fraud risk mitigations
5.0 Recommendation and way forward
6.0 Summary of Current Risk Status

Department/Unit: .....
Fraud Risk Management Quarterly Implementation Report for the Quarter Ending..... Prepared by: ..... Date: .....

Fraud Risk title & ID (From Fraud Risk Register in priority order)	**Proposed Treatment/Control Options** (From Fraud Risk Register)	**Person Responsible for Implementation of Treatment Options** (As mentioned in the Fraud Risk Register	**Timetable for Implementation** (Give specific start and end dates)	**How will this fraud risk and treatment options be monitored**	**Status of Implementation** (Completed, on-going, not done)	**Remarks and/or Comments**