

**PUBLIC SECTOR INTERNAL
CONTROL GUIDELINES**

AUGUST 2024

FOREWORD

Public sector entities regardless of size, maturity or their mandate have an evolving risk landscape arising from a volatile operating environment that is increasingly complex, technology driven and global. The need for effective utilization and safeguarding of public resources cannot be overemphasized. Consequently, design and implementation of an effective internal control system is paramount in line with the spirit of the Constitution of Kenya, 2010 as espoused in Article 10, 201 and 232. These articles require openness, accountability, efficient, effective and economic use of resources. Further, the Public Finance Management Act, 2012 and Regulations, 2015 require that each Public Entity maintains an effective system of internal control.

Designing, implementing and operating an effective internal control system can be challenging due to rapid changes in the operating environment requiring entities to be agile in responding to the changes. These guidelines are aimed at providing an understanding of what constitutes an internal control system and the insight into when internal control is being applied effectively. Further, the guidelines provide practical guidance on design, implementation, and evaluation of an internal control system.

Internal control systems in public entities should be understood within the context of the specific mandate of the entity. Therefore, the guidelines allow flexibility in designing and implementing internal control principles that can be applied at all levels of the entity. These guidelines are not intended to limit or interfere with duly granted authority related to developing legislation, rule-making, or other discretionary policy-making in an entity.

These guidelines do not provide detailed policies, procedures and practices for implementing internal control, but rather provide a broad framework within which entities can develop such detailed controls.

All public entities are required to implement an effective internal control system as per these guidelines which should be reviewed on a regular basis in response to the changing operating environment.

Contents

FOREWORD.....	1
OVERVIEW/EXECUTIVE SUMMARY.....	3
1.0. CHAPTER ONE: INTRODUCTION.....	4
1.1. Background.....	4
1.2. Purpose.....	4
1.3. Definitions of Internal Control.....	5
1.4. Benefits of Internal Control.....	6
1.5. Limitations of Internal Control.....	6
1.6. Legal and Policy Framework.....	7
1.7. Leading practices on Internal Control Framework.....	8
1.8. Applicability.....	9
1.9. Effective Date and Review.....	9
2.0. CHAPTER TWO: COMPONENTS AND PRINCIPLES OF INTERNAL CONTROL.....	10
2.1. Control Environment.....	12
2.2. Risk Assessment.....	15
2.3. Control Activities.....	18
2.4. Information and Communication.....	21
2.5. Monitoring Activities.....	24
3.0. CHAPTER THREE: ROLES AND RESPONSIBILITIES FOR INTERNAL CONTROL.....	29
3.1. The Governing body.....	29
3.2. The Audit Committee.....	30
3.3. Management.....	31
3.4. Internal Audit Responsibilities in the Third Line.....	32
3.5. External Assurance Providers.....	33
3.6. Other Stakeholders.....	33
Appendix 1: Annual Control Self-Assessment Compliance Checklist.....	1
Appendix 2: References.....	1
Appendix 3: Glossary of Terms.....	0

OVERVIEW/EXECUTIVE SUMMARY

Internal control should be recognized as an integral part of each system that management uses to guide its operations. These guidelines sets out to provide a practical guide for those involved in design, implementation, reviewing and monitoring internal control systems in public sector entities through the application of the five components of internal controls and the seventeen principles supporting the components as outlined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework.

Chapter one provides the purpose for these guidelines; the rationale for public sector entities designing, implementing and monitoring internal controls systems. It further discusses the five broad generic objectives and legislative framework that establishes the overall basis for maintaining effective internal controls in all public sector entities. Further, it describes the applicability of these guidelines to public sector entities and the effective and review date.

Chapter two highlights the five components of internal control which include control environment, risk assessment, control activities, information and communication and monitoring activities. Additionally, it describes the principles and points of focus of internal control which must be effectively designed and implemented in an integrated manner.

Chapter three explores on the roles and responsibilities of the various stakeholders in implementing effective internal controls. It focuses management's attention on its responsibilities developing, implementing and continuously maintaining a positive internal control environment. It also provides the oversight role of the Governing body; responsibility of audit committee and internal auditors as a critical part of an organization's internal control structure. Finally, it discusses the role of external parties such as the external auditors and the regulators in evaluating the effectiveness of internal control systems.

1.0. CHAPTER ONE: INTRODUCTION

1.1. Background

The global concept of internal controls gained more prominence in finance and corporate governance affairs after reported cases of financial scandal and dubious accounting practices as in the instance of Enron and dissolution of Arthur Andersen LLP. The scandals resulted into a web of reforms, including a development of new regulations and legislations such as the Sarbanes-Oxley Act (2002) which is aimed at strengthening controls in financial reporting. A famous cited global case on the effect of weak controls on corporate performance is the famous Greece debt crisis that led to the downfall of the Greece's economy as a result of massive tax evasions that ran for decades. The Greece's economy has taken more than a decade for to gain its foothold.

Locally, there has been a wide range of legislative, regulatory and policy reforms in relation to internal controls. A number of reforms are pervasive, while others are specific to operational areas such as finance, human resources, procurement among other. In spite of the many reforms, there have been many cited cases that indicate a general weak control environment in the public sector that may lead to loss of resources.

In the Systems Review as reported in the Ethics Anti-Corruption Commission's 2022-2023 Annual Report, the Commission highlighted areas of weak controls in select public entities. The areas include irregular variation of contracts, failure to establish Public Finance Management Standing Committees, prolonged delays in payment of salaries, lack of internal control documents, non-automation, failure to collect of revenues, delay in surrender of imprests, irregular payments, poor contract administration, incomplete financial records, among other. The Auditor General and the Controller of Budget reports underscore that lack of effective controls across public sector entities largely contributes to poor implementation of projects, ballooning of pending bills, poor resource mobilization and leakages in the collection of own source revenue. This renders the effective and efficient discharge entities' mandate difficult. As concluded by a local researcher (Omolo, 2018), the performance of Ministries in the Government of Kenya (public sector entities) and internal controls are positively correlated. Therefore, the centrality of internal control on performance management and service delivery cannot be understated.

1.2. Purpose

Public entities are continually seeking ways to achieve their mandate and improve accountability to stakeholders. Entities set strategies that support their missions and visions and set objectives at different levels to achieve respective mandates. The purpose of these guidelines is to provide public entities with a practical approach to design, implement, monitor and continually improve internal control systems. The guidelines have been developed to guide management in designing and implementing, and Governing bodies in oversighting effective internal control systems in the following areas among others:

- i. Provide an overall framework for establishing and maintaining effective internal controls.
- ii. Provide a principle-based approach that allows flexibility in designing and implementing internal control principles that can be applied at the entity, and functional levels.
- iii. Provide an opportunity to expand the application of internal control beyond financial reporting to other forms of reporting, operations, and compliance objectives.

- iv. Provide an opportunity to eliminate ineffective, redundant, or inefficient controls that provide minimum value in reducing risks to the achievement of entity's objectives.
- v. Describe internal control roles and responsibilities for public sector entities.
- vi. Describe common internal control practices.
- vii. Provide references for guidance in implementing internal control frameworks and capacity building

Additionally, the guidelines will provide greater confidence to external stakeholders with regard to the entity's ability to identify, analyze and respond to risk and changes in the operating environment. Further, the guidelines will provide a better understanding of the requirements of an effective internal control system.

The guidelines will enable entities to effectively and efficiently develop internal control systems that adapt to changing operating environments, mitigate risks to acceptable levels, and support sound decision making and governance of the entities.

Internal control means a set of systems to ensure that financial and other records are accurate, reliable, complete and ensure adherence to the management policies of the Ministry, department or other agency of Government, for the orderly and efficient conduct of the Ministry, department or agency, and the proper recording and safeguarding of its assets and resources. (PFM Regulations, 2015).

1.3. Definitions of Internal Control

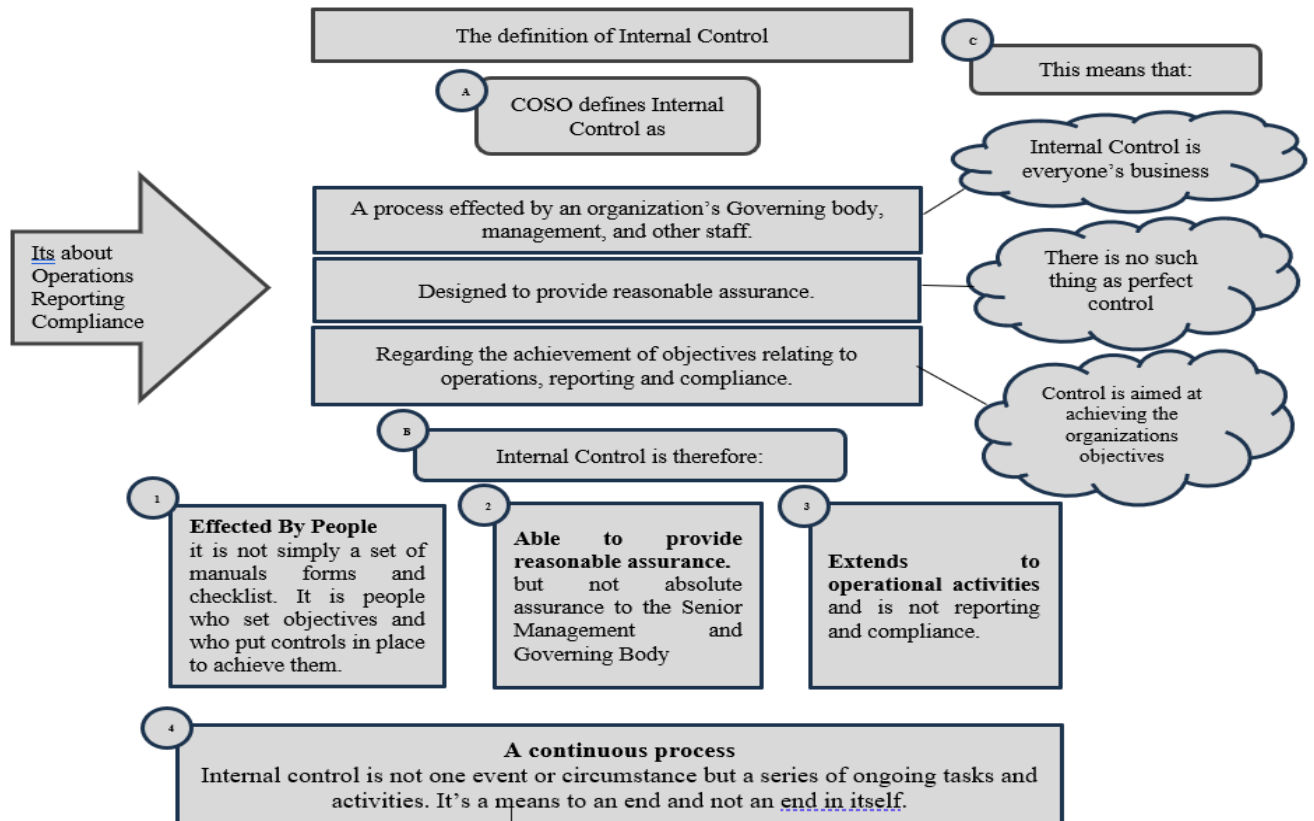
Internal control is a **process** effected by an entity's **Governing body, Management** and other personnel, designed to provide reasonable assurance regarding the **achievement of objectives** relating to operations, reporting and compliance. Internal control helps entities achieve important objectives and sustain and improve performance. (COSO Internal Control – Integrated Framework, 2013).

The 2013 COSO Framework is designed to be used by entities to assess the effectiveness of the system of internal control to achieve the following objectives;

1. Operations - These pertain to effectiveness and efficiency of the entity's operations, including operational and financial performance goals, and safeguarding assets against loss.
2. Reporting Objectives -These pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the entity's policies.
3. Compliance Objectives - These pertain to adherence to laws and regulations to which the entity is subject.

The terms defining internal control are elaborated in *Figure 1* below.

Figure 1: Definition of Internal Control



1.4. Benefits of Internal Control

The benefits of an effective control system include but are not limited to;

- i. Alignment of an organization's employees, partners, and stakeholders with its commitment to purpose and articulated objectives.
- ii. Enhanced data quality, utility, comparability, and reliability.
- iii. Strengthened ability to support operations and compliance objectives.
- iv. Better-informed decision making by internal management, external investors, and other stakeholders.
- v. Enhanced understanding of risks and the ability to mitigate them.
- vi. Greater overall market efficiency.
- vii. Increased access to and lowered cost of capital.

1.5. Limitations of Internal Control

System of internal control cannot prevent poor judgement or decisions, or external events that can cause entities to fail in achieving its goals. Limitations may result from but not limited to:

- i. Suitability of objectives established as a precondition to internal controls.
- ii. Changes in the legislative, and policy frameworks;
- iii. Human related factors e.g. fatigue, bias, errors, negligence, and distractions;
- iv. Overriding internal controls and Circumventing controls through collusion;
- v. Resources/staff limitations
- vi. Changes in technology, and
- vii. External events beyond an entities control.

Notwithstanding the limitations above entities should design an Internal control system that minimises their impact on realisation of strategic objectives.

1.6. Legal and Policy Framework

The promulgation of the Constitution of Kenya, 2010, resulted into reforms to promote performance and accountable governance in public sector. As part of the public financial management reforms, the government has over the years enacted various legislations to promote governance, risk management and control processes throughout the public sector. Implementing an effective entity internal control system will support the requirements of:

i. The Constitution of Kenya, 2010

Implementation of an effective internal control system is in line with the spirit of the Constitution as espoused in Article 10, 201 and 232 that requires openness, accountability, efficient, effective and economic use of resources, transparency and provision to the public of timely and accurate information.

ii. The Public Finance Management Act, 2012 and Regulations 2015

Implementation of an effective internal control system helps accounting officer to comply with PFM Act, 2012 section 68 in ensuring resources are used in a way that is lawful and authorized: and effective, efficient, economical and transparent manner. The regulation provides:

Regulations 165(1) (b)/158 (1) (b) of the National/County Government PFM Act regulations, 2015, requires the Accounting Officer to ensure that the national/county government entity develops a system of risk management and internal controls that build robust business operations.

Regulations 175/168 of the National/County Government PFM Act regulations, 2015, requires the audit committee to support the Accounting Officers with regard to their responsibilities for issues of risk, control and governance and associated assurance provided that the responsibility over the management of risk, control and governance processes remains with the management of the concerned entity.

The Audit Committee Guideline (Gazete Notice No. 2690/91 of 2016) for national and county government provide for the Audit committee to review the entity financial controls while management is responsible for identification, assessment, mitigating and monitoring of risk.

iii. Mwongozo - The Code of Governance for State Corporations 2015

Mwongozo – The code of governance requires governing bodies to maintain adequate systems and processes of accountability, risk management and internal control. The Governing body delegates to management the responsibility of designing, implementing and monitoring the effectiveness of internal control systems.

1.7. Leading practices on Internal Control Framework

Leading practices on internal control include but not limited to;

i. COSO Internal Control–Integrated Framework 2013 inclusive of updates thereto (The Committee of Sponsoring Organizations of the Treadway Commission’s internal control framework)

COSO’s Internal Control – Integrated Framework was introduced in 1992 as guidance on how to establish better controls so companies can achieve their objectives with minimal surprises. COSO categorizes entity-level objectives into operations, financial reporting, and compliance. The revised 2013 framework includes 17 basic principles representing the fundamental concepts associated with its five components: control environment, risk assessment, control activities, information and communication, and monitoring. Some of the principles include key elements for compliance, such as integrity and ethical values, authorities and responsibilities, policies and procedures, and reporting deficiencies.

ii. COBIT 2019: Control Objectives for Information and Related Technology (Information Systems Audit and Control Association’s IT Governance framework)

COBIT is an internationally accepted controls-based framework for IT governance that was first released by ISACA in 1996. COBIT has 34 high-level processes that cover 210 control objectives categorized in four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring and evaluation.

The framework guides an organization on how to use IT resources (i.e., applications, information, infrastructure, and people) to manage IT domains, processes, and activities to respond to business requirements, which include compliance, effectiveness, efficiency, confidentiality, integrity, availability, and reliability. Well-governed IT practices can assist businesses in complying with laws, regulations, and contractual arrangements.

iii. ISO: International Organization for Standardization

ISO has developed more than 16,000 international standards for stakeholders such as industry and trade associations, science and academia, consumers and consumer associations, governments and regulators, and societal and other interest groups. The ISO 9001 of 2015 series focuses on quality management systems, including ensuring controls are in place to comply with applicable regulatory requirements. The ISO 14001 series of 2015 focuses on environmental management systems, including complying with applicable environmental regulatory requirements. The ISO 27001 series of 2018 focuses on information security management systems. The 27001 series helps organizations establish information security standards that meet business needs while ensuring compliance with regulatory and contractual requirements.

1.8. Applicability

The internal control guidelines have been developed to guide all public entities in developing Internal Control Systems that should be tailored to their specific environments. The guidelines are based on principles which guide on the characteristics of effective internal control systems. Public sector entities should in addition to these guidelines comply with internal control frameworks issued by their respective industry regulators.

1.9. Effective Date and Review

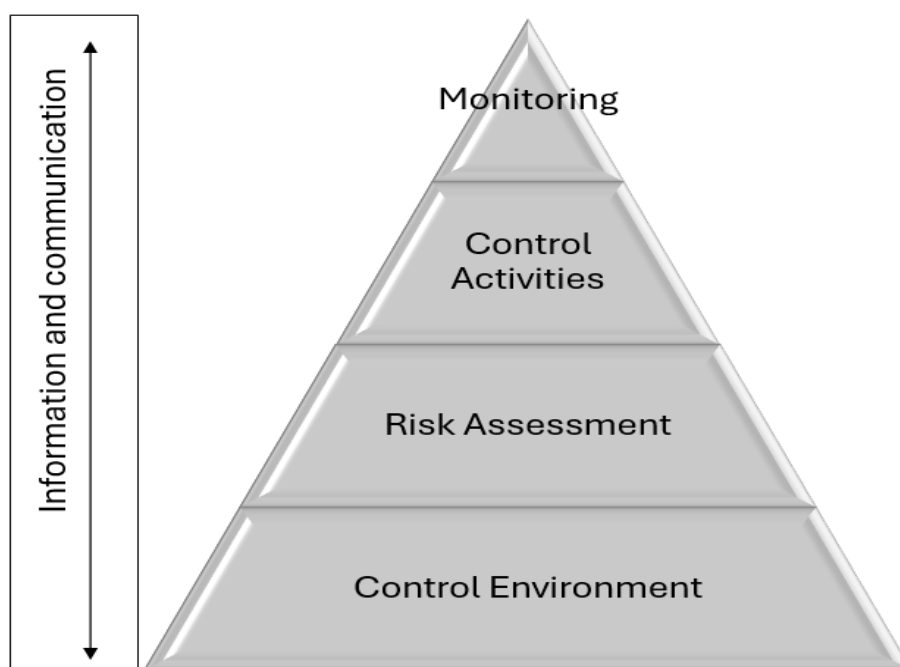
These guidelines shall be effective on the date approved. The guidelines take into account the latest international developments in internal control and shall be reviewed every three years or when circumstances dictate.

DRAFT

2.0. CHAPTER TWO: COMPONENTS AND PRINCIPLES OF INTERNAL CONTROL

The Chapter elaborates the five components namely: control environment; risk assessment; control activities; information and communication; and monitoring; and seventeen principles that are requisite to an effective internal control system. For the internal controls to be considered effective all the five components and relevant principles should be present, functioning and operating together in an integrated manner.

Internal control is an integral process that is continuously adapting to the changes a public sector entity faces. Management and staff at all levels have to be involved in this process to address risks and provide reasonable assurance on the achievement of the public sector entity's mission and general objectives.



Management should develop action points to demonstrate how each of the five components of internal control framework are achieved annually. COSO Internal control – integrated framework describes a direct relationship between objectives, (what an entity strives to achieve), components (what is required to achieve the objectives) and the organizational structure of the

entity (the operating units, legal entities, and other). The relationship can be depicted in the form of a cube described in *Figure 2* below.



Figure 2, Source: COSO Internal Control – Integrated Framework 2013

Control Environment

1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority, and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability.

Risk Assessment

6. Specifies suitable objectives
7. Identifies and analyses risk
8. Assesses fraud risk
9. Identifies and analyses significant change

Control Activities

10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys control activities through policies and procedures

Information and Communication

13. Uses relevant information
14. Communicates internally
15. Communicates externally

Monitoring Activities

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

Consistent with the COSO framework, these Guidelines features five components and seventeen principles for integrated and effective internal control as listed below:

2.1. Control Environment

The control environment is the foundation for an internal control system. It provides the discipline and structure, which affect the overall quality of internal control. It influences how objectives are defined and how control activities are structured. The Governing body and management establish and maintain an environment throughout the entity that sets a positive attitude toward internal control. The key principles and points of focus relating to control environment include:

Principle	Points of Focus	Demonstrate Conformance
1. The organization demonstrates a commitment to integrity and ethical values.	Tone at the top	The Governing body and management: <ul style="list-style-type: none"> a) Demonstrates the importance of integrity and ethical values through their directives, attitudes, and behavior. b) Leads by example that demonstrates the entity's values, philosophy, and operating style. c) Reinforces the commitment to doing what is right, not just maintaining a minimum level of performance necessary to comply with applicable laws and regulations, so that these priorities are understood by all stakeholders, such as regulators, employees, and the general public. d) Takes appropriate action when deviations occur. e) Establishes and operationalizes an effective internal audit function as part of the internal control system.
	Standard of Conduct	The Governing body and management: <ul style="list-style-type: none"> a) Defines the organization's expectations of ethical values in the standards of conduct, code of conduct, or guidelines. b) Ensures staff sign, understand and adherence to codes.
	Adherence and deviations to Standard of Conduct	<ul style="list-style-type: none"> a) Management establishes and implements an effective whistle blowing program. b) Management or assurance providers evaluate adherence to code of conduct through conducting investigations on reported violations. c) Deviations are corrected in a timely and consistent manner.
2. The Governing body Demonstrates independence from management and exercise	Establishes Oversight Responsibilities	<ul style="list-style-type: none"> a) An entity determines an oversight structure to fulfill responsibilities set forth by applicable laws and regulations, relevant government circulars, and feedback from key stakeholders. b) The entity adopts a Charter that clearly outlines roles and responsibility of Governing body that are distinct from management.

Principle	Points of Focus	Demonstrate Conformance
oversight of the development and performance of internal control.	Independence and relevant expertise	a) The governing body is independent from management and demonstrates relevant skills and expertise in carrying out its oversight responsibilities. Independence is demonstrated in the board member's objectivity of mind, action, appearance, and fact. b) Board members avoid/declare conflict of interest.
	Oversight for the internal control system	a) The governing body is responsible for oversight of management's design, implementation, and performance of internal controls. b) The governing body establishes effective Board committees to oversight internal control.
3. Management, with Board oversight establishes structures, reporting lines and appropriate authorities and responsibilities in the pursuit of objectives.	Organizational Structure	a) The entity establishes an organizational structure with clearly defined roles and responsibilities. b) Management considers the entity's overall responsibilities to stakeholders and establishes reporting lines that allow the entity to both communicate and receive information from stakeholders. c) Management periodically reviews and evaluates the structures for continued relevance and effectiveness and efficiency in support of the internal control system. d) Management reviews of the structure to align with organization strategy.
	Authorities and Responsibilities	a) The Governing body delegates authority and defines and assigns responsibility to management. b) Management considers the overall responsibilities assigned to each function and, determines what key roles are needed to fulfill the assigned responsibilities. c) Authority and responsibility are delegated based on demonstrated competence, and roles are defined based on who is responsible for or kept informed of decisions. d) The entity defines reporting lines at all levels
	Documentation of the Internal Control System	Management develops and implements policies and procedure manuals and maintains documentations of its internal control system and reviews in line with operating environment.
4. The organization demonstrates a commitment to attract, develop and retain competent individuals in	Expectations of Competence	a) Management develops and implements Human Resource Instruments b) The oversight body evaluates the competence of entity management. c) Management establishes expectations of competence for all staff through policies within the entity's internal control system to enable the entity achieve its objectives.

Principle	Points of Focus	Demonstrate Conformance
<p>alignment with objective</p>		<p>d) Management considers standards of conduct, assigned responsibility, and delegated authority.</p> <p>e) Management holds individuals accountable to established policies by evaluating competence. This is integral to attracting, developing, and retaining staff.</p> <p>f) Management acts as necessary to address any deviations from the established policies.</p>
	<p>Recruitment Development and Retention of staff</p>	<p>a) The entity Human Resource instruments documents the policies and procedures on recruitment, development, mentor and retention of staff.</p> <p>b) Management recruits, develops, and retains competent personnel to achieve the entity's objectives.</p>
	<p>Succession and Contingency Plans</p>	<p>a) Management defines succession and contingency plans for key roles to help the entity continue achieving its objectives.</p> <p>b) Management defines contingency plans for assigning responsibilities if a key role in the entity is vacated without advance notice. The importance of the key role in the internal control system and the impact to the entity of its vacancy dictates the formality and depth of the contingency plan.</p> <p>c) Management trains succession candidates to assume the key roles.</p> <p>d) Where an entity places considerable reliance on an external party contingency plans will be required to ensure continuity of services.</p>
<p>5. The entity holds staff accountable for their internal control responsibilities in the pursuit of objectives.</p>	<p>Enforcement of Accountability</p>	<p>a) The entity's effective Performance management system takes into account responsibility for internal controls.</p> <p>b) Accountability for performance of internal control responsibility supports day-to-day decision making, attitudes, and behaviors.</p> <p>c) The oversight body holds management accountable as well as the entity as a whole for its internal control responsibilities.</p> <p>d) Management, with oversight from the Governing body, takes corrective action as necessary to enforce accountability for internal controls in the entity.</p>
	<p>Performance measures, incentives and rewards</p>	<p>a) Management establishes an appropriate reward and sanction policy.</p> <p>b) Management with oversight of Governing body establish performance measures, incentives, and other rewards appropriate for internal control responsibilities at all levels of the entity, considering the achievement of both short-term and longer-term objectives.</p>

Principle	Points of Focus	Demonstrate Conformance
		c) Management evaluates incentives so that they align with the entity's standards of conduct.
	Consideration of Excessive Pressures	a) Management continuously monitors agreed performance targets. b) Management with oversight from governing body evaluates and adjusts pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance. c) Management adjusts excessive pressures using many different tools, such as rebalancing workloads or increasing resource levels in accordance with the entity's standards of conduct.

2.2. Risk Assessment

Risk is defined as the effect of uncertainty on objectives. Every entity faces a variety of risks from external and internal sources. Risk assessment is a dynamic and iterative process of identifying and analyzing relevant risks to the achievement of the entity's objectives and determining the appropriate response. Public sector entities are encouraged to refer to Public Sector Risk Management guidelines issued by Public Sector Accounting Standards Board (PSASB). The key principles relating to risk assessment include:

Principle	Points of Focus	Demonstrate Conformance
6. The entity sets clear objectives to enable the identification and assessment of risks relating to objectives.	Operations Objectives	a) Management implements a risk management framework that is integrated with day-to-day operations. b) Management uses operations objectives as a basis for allocating resources needed to attain desired performance level while taking into account acceptable levels of risks. c) Measurable objectives are also stated in a quantitative or qualitative form that permits reasonably consistent measurement. d) Management evaluates and, if necessary, revises defined objectives so that they are consistent with these requirements and expectations. This consistency enables management to identify and analyze risks associated with achieving the defined objectives.
	Reporting Objectives	Reporting objectives pertain to the preparation of reports that encompass reliability, timeliness, transparency, or other terms as set forth by regulators, standard-setting bodies, or by the entity's policies as set out by the Governing body. This category includes external and internal financial reporting and operational reporting.
	Compliance Objectives	Management sets compliance objectives that guide minimum standards of conduct based on applicable laws and regulations.

Principle	Points of Focus	Demonstrate Conformance
<p>7. The entity identifies risks to the achievement of its objectives and the risks are analyzed so as to determine how the risks should be managed.</p>	Risk Identification	<p>a) Management considers the types of risks that impact the entity positively or negatively at all levels when identifying risks,.</p> <p>b) Risk identification considers both external and internal impact in achievement of the entity's objectives.</p> <p><i>NB: Further information is provided in public sector risk management guidelines.</i></p>
	Risk analysis	<p>a) The governing body may oversee management's estimates of significance so that risk tolerances are properly defined.</p> <p>b) Management analyzes the identified risks to estimate their significance, assess their effect on achieving the defined objectives at all levels of the entity and provide a basis for designing internal controls.</p> <p>c) Management analyses the risks by considering the magnitude of impact and likelihood of occurrence.</p> <p>d) Risks may be analyzed on an individual basis or grouped into categories with related risks and analyzed collectively.</p> <p>e) Management considers the correlation among different risks or groups of risks when estimating their significance. The specific risk analysis methodology used can vary by entity because of differences in entities' missions and the difficulty in qualitatively and quantitatively defining risk tolerances.</p>
	Risk evaluation	<p>a) Management evaluates risks to assist in making decisions on which risk need treatment and the priority for treatment implementation.</p> <p>b) Management compares the results of the risk assessment with the risk criteria / risk appetite to determine whether the risk and/or its magnitude is acceptable or tolerable or whether additional action is required.</p>
	Risk Response	<p>a) Risk responses include: pursue opportunity, tolerate/acceptance, terminate/avoidance, treatment/reduction/mitigate and transfer/sharing.</p> <p>b) Based on the selected risk response, management designs the specific actions to respond to the analyzed risks. The nature and extent of risk response actions depend on the defined risk tolerance.</p> <p>c) Operating within the defined risk tolerance provides greater assurance that the entity will achieve its objectives when risk response actions do not enable the entity to operate within the defined risk tolerances, management may need to revise risk responses or reconsider defined risk tolerances.</p> <p>d) Management conducts periodic risk assessments to evaluate the effectiveness of the risk response action.</p>

Principle	Points of Focus	Demonstrate Conformance
<p>8. The entity to consider the potential for fraud in assessing risks to the achievement of objectives.</p>	Types of Fraud	<p>a) Management considers what can occur within the entity to provide a basis for identifying fraud risks. Fraud can be categorized as follows:</p> <ul style="list-style-type: none"> i. Fraudulent reporting ii. Misappropriation of entity's assets iii. Corruption <p>b) Management considers in addition to fraud, other forms of misconduct that can occur, such as waste of resources, abuse of office, bribery, misuse of authority or position for personal gain.</p>
	Fraud Risk Factors	<p>a) Management establishes and continually improve anti-fraud mechanism such as whistle blowing program.</p> <p>b) Fraud risk factors include the following:</p> <ul style="list-style-type: none"> i. Incentive/pressure - financial or social pressure pushing an individual towards committing fraud. Pressures can include money problems, gambling, debts, alcohol, drug addiction or. ii. Opportunity - Circumstances exist, such as the absence of control or ineffective controls. iii. Attitude/rationalization - personal justification of dishonest action. iv. Capability - refers to the personal traits and ability of persons that enable them to perpetrate fraud, beyond the environmental or situational factors of opportunity, rationalization and pressure. This includes a person's knowledge of the policies, procedures and controls of the entity and ability to override controls.
	Response to Fraud Risks	<p>a) Management establishes and continually improve anti-fraud mechanism such as whistle blowing program.</p> <p>b) Management designs an overall risk response and specific actions for responding to fraud risks. It may be possible to reduce certain fraud risks by making changes to the entity's activities and processes.</p>
<p>9. The entity identifies and assesses changes that could significantly impact the system of internal control.</p>	Identification of Change	<p>a) Management implements an effective Risk Management Framework that requires regular assessment of operating environment to identify changes that could impact internal control system.</p> <p>b) Management identifies, on a timely basis, significant changes to internal and external conditions that have already occurred or are expected to occur.</p> <p>c) Management communicates identified significant across the entity through established reporting lines to appropriate staff.</p>

Principle	Points of Focus	Demonstrate Conformance
	Analysis of and Response to Change	a) Management implements an effective Risk Management Framework that requires regular assessment of operating environment to inform responses. b) Management analyzes the identified changes and their effects on the internal control system and responds by revising the internal control system on a timely basis, as and when necessary, to maintain its effectiveness. c) Further, changing conditions often prompt new risks or changes to existing risks that need to be assessed. As part of analyzing and responding to change, management performs a risk assessment to identify, analyze, evaluate and respond to any new risks prompted by the changes.

2.3. Control Activities

Control activities are the policies and procedures established to respond to risks and to achieve the entity's objectives. To be effective, control activities must be appropriate, function consistently according to plan throughout the period, and be cost effective, comprehensive, reasonable and directly relate to the control objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of the following activities;

- i. Directive: These are actions taken to encourage a desirable event to occur. Examples include: organizational structure, policies and procedures, monthly bank reconciliations
- ii. Preventive controls aim to decrease the chance of fraud and error before they occur. Examples include; authorization, approval, segregation of duties, access controls
- iii. Detective controls activities designed to discover unintended event or result. Examples include; verifications, reconciliation and reviewing of operating performance.
- iv. Corrective are activities designed to remedy undesirable events that have already occurred. Examples include disciplinary procedures, training, and post balance sheet date adjustments.

Entities should reach an adequate balance between detective and preventive versus detective and corrective control activities. Where the management is unable to implement primary controls the management should implement compensating controls. These are alternative means of providing assurance that an organization's objectives will be achieved, especially when other controls are not sufficient for example where Segregation of Duties is not possible supervision would be adequate. Entities need to continuously review their controls to assess their relevance. The key principles relating to control activities include:

Principle	Points of Focus	Demonstrate Conformance
10. The entity develops control activities that contribute to risk response	Integration with Risk Assessment	Management designs control activities in response to the entity's objectives and risks to achieve an effective internal control system. This entails maintenance of risk registers that incorporate entity's objectives, risks and controls.

Principle	Points of Focus	Demonstrate Conformance
<p>to acceptable levels.</p>	<p>Design of Appropriate Types of Control Activities</p>	<p>a) Management designs appropriate types of control activities (directive, preventive, detective and corrective) for the entity's internal control system.</p> <p>b) Control activities help management fulfill responsibilities and address identified risk responses in the internal control system.</p> <p>c) Control activities can be implemented in either an automated or a manual manner.</p>
	<p>Design of Controls Activities at Various Levels</p>	<p>a) Management considers how the environment complexity, nature and scope of its operations as well as the specific characteristics of its organization affect the selection and development of control activities.</p> <p>b) In designing internal controls management considers the various levels as below:</p> <p>i. Entity-level: are controls designed by the management and endorsed by the governing body e.g policies and procedures</p> <p>ii. Functional/Operational level: actions built in operational unit level that support entity level and operating levels strategies e.g authorization and approval, supervision</p>
	<p>Segregation of Duties</p>	<p>a) Management should Identify related-tasks in every business process. The tasks should be assigned to different officers to reduce the risk of error or inappropriate or fraudulent action. Caution should be taken to avoid duplication or creation of unnecessary bureaucracies.</p> <p>b) Management override circumvents existing control activities and increases fraud risk. Management addresses this risk through segregation of duties but cannot absolutely prevent it because of the risk of collusion.</p> <p>c) Management considers the need to separate control activities related to authority, custody, and recording of operations to achieve adequate segregation of duties. In particular, segregation of duties can address the risk of management override.</p> <p>d) Segregation of duties helps prevent fraud, waste, and abuse in the internal control system.</p>
<p>11. The entity selects and develop general control activities over technology to</p>	<p>Design of Entity's Information System</p>	<p>a) Management designs the entity's information system to respond to the entity's objectives and risks.</p> <p>b) An information system is the people, processes, data, and technology that management organizes to obtain, communicate, or dispose of information. It includes both manual and technology-enabled information processes.</p>

Principle	Points of Focus	Demonstrate Conformance
<p>support the achievement of objectives</p>		<p>c) Information systems may enhance internal control over confidentiality, integrity and availability of information by appropriately restricting access.</p>
	<p>Design of Appropriate Types of Control Activities</p>	<p>a) Management designs general and application control activities that support the entity's objectives;</p> <p>i. General controls are the policies and procedures that apply to all or a large segment of an entity's information systems. E.g security management, logical and physical access, configuration management, segregation of duties, and contingency planning.</p> <p>ii. Application controls, are those controls that are incorporated directly into computer applications to achieve validity, completeness, accuracy and confidentiality of information and data during application processing. This includes; input controls , processing and output controls.</p>
	<p>Design of Information Technology Infrastructure</p>	<p>a) Management evaluates the objectives of the entity and related risks in designing control activities for the information technology infrastructure.</p> <p>b) Management designs control activities over the information technology infrastructure to support the completeness, accuracy, and validity of information processing by information technology.</p> <p>c) Information technology requires an infrastructure in which to operate, including communication networks for linking information technologies, computing resources for applications to operate, and electricity to power the information technology. An entity's information technology infrastructure can be complex. It may be shared by different units within the entity or outsourced either to service organizations or to location-independent technology services. Examples includes BCP/DRP plans. (ICTA)</p>
	<p>Design on Security Management</p>	<p>a) Management designs control activities for security management of the entity's information system for appropriate access by internal and external sources. Objectives for security management include confidentiality, integrity and availability</p> <p>b) Security management includes access rights across various levels of data, operating system, network, application, cryptographic controls and physical controls.</p>
	<p>Design of Information Technology Acquisition, Development,</p>	<p>a) Management evaluates the objectives and risks of the technology adopted in designing control activities over its system development methodology.</p>

Principle	Points of Focus	Demonstrate Conformance
	and Maintenance	<ul style="list-style-type: none"> b) Methodologies that may be used include but not limited to Rapid Application development, Prototyping, Agile development, Spiral, & Object oriented systems development c) The controls may include authorization of change requests; reviewing the changes, approvals, and testing results; and designing protocols to determine whether changes are made properly.
12. The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.	Documentation of Policies and Procedures	<ul style="list-style-type: none"> a) Management formulates policies which shall be approved by the governing body. b) Those in key roles for the unit may further define policies through day-to-day procedures, depending on the rate of change in the operating environment and complexity of the operational process. Procedures may include the timing of when a control activity occurs and any follow-up corrective actions to be performed by competent staff if deficiencies are identified. c) Management communicates to staff the policies and procedures to implement the control activities for their assigned responsibilities.
	Periodic Review of Control Activities	<ul style="list-style-type: none"> a) Management periodically reviews policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks. b) Changes may occur in staff, operational processes, or information technology as a result of changes in legislation that may have an impact in an entity's objectives.

2.4. Information and Communication

Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control. For example, one of the objectives of internal control is fulfilling public accountability obligations. This can be achieved by developing and maintaining reliable and relevant financial and non-financial information and communicating this information by means of a fair disclosure in a timely manner.

Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is how information is disseminated throughout the entity. It enables staff to receive a clear message from senior management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations.

Stakeholders' ability to make appropriate decisions is affected by the quality of information which implies that the information should be appropriate, timely, current, accurate and accessible. Information may be communicated in order to comply with laws and regulations. The key principles relating to information and communication include:

Principle	Points of Focus	Demonstrate Conformance
<p>13. The entity obtains or generates and uses relevant, reliable and quality information to support the functioning of internal control.</p>	<p>Identification of Information Requirements</p>	<p>a) Management defines the identified information requirements at the relevant level for appropriate staff. As change in the entity's objectives and risks occurs, management adjusts information requirements to meet modified objectives and address risks.</p> <p>b) For example management may perform an annual entity-wide survey of its employees to gather information .The survey is part of a process that produces information to support the control environment component and may also provide input into the selection, development, implementation or maintenance of control activities.</p>
	<p>Relevant Data from Reliable Sources</p>	<p>a) Management evaluates both internal and external sources of data for reliability and relevance.</p> <p>b) Relevant data has a logical connection with, the identified information requirements. Reliable data is reasonably free from error and bias. Sources of data can be operational, financial, or compliance related.</p> <p>c) Management obtains data on a timely basis so that they can be used for effective monitoring.</p> <p>d) Information meets the requirements when relevant data from reliable sources is used.</p>
	<p>Data Processed into Quality Information</p>	<p>a) Management processes data to ensure that the information generated by the entity is complete, accurate, reliable, timely and accessible. The controls may include internal quality reviews, process and output controls, dissemination.</p> <p>b) Management uses the quality information to make informed decisions and evaluate the entity's performance in achieving key objectives and addressing risks.</p>
<p>14. The entity internally communicates information, including objectives and responsibilities for internal</p>	<p>Communication throughout the Entity</p>	<p>a) Management communicates quality information throughout the entity using established reporting lines.</p> <p>b) A process is in place to communicate required information to enable all staff to understand and carry out their internal control responsibilities.</p> <p>c) Communication exists between management and the governing body of directors so that both have information</p>

Principle	Points of Focus	Demonstrate Conformance
<p>control, necessary to support the functioning of internal controls.</p>		<p>needed to fulfill their roles with respect to the entity's objectives.</p> <p>d) Separate communication channels, such as whistle-blowing mechanisms, are in place to enable anonymous or confidential communication when normal channels are ineffective.</p>
	<p>Appropriate Methods of Communication</p>	<p>a) Management periodically evaluates the entity's methods of communication so that it has the appropriate tools to communicate quality information on a timely basis. For example, communication policy.</p> <p>b) Management considers a variety of factors in selecting an appropriate method of communication. Some factors to consider:</p> <ul style="list-style-type: none"> i. Audience - The intended recipients of the communication ii. Nature of information - Purpose and type of information iii. Availability - Information readily available to the audience iv. Cost - The resources used to communicate the information v. Legal or regulatory requirements - Requirements in laws and regulations that may impact communication.
<p>15. The entity communicates with external parties regarding matters affecting the functioning of internal control</p>	<p>Communication with External Parties</p>	<p>a) Management evaluates the entity's methods of communication with external parties through approved reporting lines so that external parties can help the entity achieve its objectives and address related risks.</p> <p>b) Management institutes processes to communicate relevant and timely information to external parties including but not limited to regulators, legislators, external auditors, and any other stakeholders.</p> <p>c) Relevant information resulting from assessments conducted by external parties is communicated to the governing body.</p> <p>d) Separate communication channels, such as whistle-blowing mechanisms, are in place to enable anonymous or confidential communication when normal channels are ineffective.</p>
	<p>Appropriate Methods of Communication</p>	<p>a) Management periodically evaluates the entity's methods of communication so that it has the appropriate tools to communicate quality information on a timely basis. For example communication policy.</p>

Principle	Points of Focus	Demonstrate Conformance
		b) Management considers a variety of factors in selecting an appropriate method of communication. Some factors to consider: <ul style="list-style-type: none"> i. Audience - The intended recipients of the communication ii. Nature of information - Purpose and type of information iii. Availability - Information readily available to the audience iv. Cost - The resources used to communicate the information v. Legal or regulatory requirements - Requirements in laws and regulations that may impact communication.

2.5. Monitoring Activities

Monitoring activities assess whether each of the five components of internal control and relevant principles is present and functioning. Monitoring is a key input of the entity's assessment of the effectiveness of internal control. It also provides valuable support for point of focus the effectiveness of the system of internal control.

The entity uses ongoing, separate evaluations, or combination of the two, to ascertain whether the components of internal control (including controls to effect principles across the entity and its subunits) are present and functioning.

i. Ongoing evaluations

Ongoing evaluation of internal control is built into the normal recurring operating activities of an entity. It includes regular management and supervisory activities and other actions staff take in performing their duties.

Ongoing evaluation activities cover each of the internal control components and involve action against irregular, unethical, uneconomical, inefficient and ineffective internal control systems.

ii. Separate evaluations

Separate evaluations cover the evaluation of the effectiveness of the internal control system and ensure that internal control achieves the desired results based on predefined methods and procedures.

Separate evaluations provide greater objectivity when performed by reviewers who do not have direct operational responsibility e.g internal auditors, monitoring and evaluation unit.

Internal control deficiencies should be reported to the appropriate level of management. Monitoring should ensure that audit findings and recommendations are adequately and promptly resolved. The key principles relating to monitoring activities include:

Principle	Points of Focus	Demonstrate Conformance
<p>16. The entity selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control systems are present and functioning.</p>	<p>Establishment of a Baseline</p>	<p>a) Management establishes a baseline to monitor the internal control system.</p> <p>b) Management may establish a baseline through control self-assessments or a predetermined industry baseline.</p> <p>c) The baseline is the minimum or starting point used for comparison for example the current state of the internal control system or relevant industry baseline.</p> <p>d) As part of monitoring, management determines when to revise the baseline to reflect changes in the internal control system.</p>
	<p>Internal Control System Monitoring</p>	<p>a) Management performs ongoing evaluations of the design and operating effectiveness of the internal control system.</p> <p>i. Ongoing evaluations includes regular management and supervisory activities, comparisons, reconciliations, and other routine actions. Ongoing evaluations may include automated tools, which can increase objectivity and efficiency by electronically compiling evaluations of controls and transactions.</p> <p>ii. Separate evaluations can employ the same techniques as ongoing evaluations, but they are designed to evaluate controls periodically and are not ingrained in the routine operations of the entity. Separate evaluations may include: internal audit evaluations, cross operating unit/functional evaluations, benchmarking/peer evaluations and self-assessments.</p> <p>b) Management selects, develops, and performs a mix of monitoring activities usually including both ongoing and separate evaluations, to ascertain whether each of the five components of internal control is present and functioning.</p>
	<p>Evaluation of Monitoring Results</p>	<p>a) Management can use the baseline as criteria in evaluating the internal control system and make changes to reduce the difference between the criteria and condition. This can be achieved through ongoing and separate evaluations.</p> <p>b) Differences between the results of monitoring activities and the established baseline may indicate internal control issues, including undocumented changes in the internal control system or potential internal control deficiencies. For example, reports from the external and internal assurance providers, complaints from the general public and regulator comments may indicate areas in the internal control that need improvement.</p>

Principle	Points of Focus	Demonstrate Conformance
		<p>c) Management either changes the design of the internal control system to better address the objectives and risks of the entity or improves the operating effectiveness of the internal control system based on changes in the entity and its environment.</p>
<p>17. The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible to take action, including senior management and Governing body.</p>	<p>Input for Remediation of internal control weaknesses</p>	<p>a) Deficiencies identified in the internal control system are reported to the governing body. b) The governing body oversees and provides direction to management on the remediation of identified control weaknesses. c) The governing body supports and ensure implementations of recommendations from assurance providers on internal controls.</p>
	<p>Reporting of internal control weaknesses</p>	<p>a) The governing body provides needed support or oversight for taking corrective action and is positioned to communicate with others in the entity whose activities may be affected. Where findings cut across organizational boundaries, the deficiencies are reported to all relevant parties to drive appropriate action. b) Staff communicate issues internally to the officer in the key role responsible for the internal control or associated process. Depending on the nature of the issues, management should consider reporting major internal control weaknesses to the governing body. c) Depending on the entity's regulatory or compliance requirements, the entity may also be required to report issues externally to appropriate external parties, such as the legislators, regulators, and standard-setting bodies that establish laws, rules, regulations, and standards to which the entity is subject.</p>
	<p>Evaluation of internal control weaknesses</p>	<p>a) Management evaluates issues identified through monitoring activities reported by staff to determine whether any of the issues measure to the level of an internal control weaknesses. b) Internal control weaknesses require further evaluation and rectification by management. An internal control weakness can be in the design, implementation, or operating effectiveness of the internal control and its related process. c) Management determines from the type of internal control weakness the appropriate corrective actions to remediate the internal control weakness on a timely basis. d) Management assigns responsibility and delegate's authority to rectify the internal control weakness.</p>
	<p>Monitoring Corrective Action</p>	<p>Management completes and documents corrective action plans to remediate internal control deficiencies on a timely basis.</p>

Principle	Points of Focus	Demonstrate Conformance
		Management, with the governing body, monitors the status of remediation efforts so that they are completed within stipulated timelines. These corrective actions may include but not limited to resolution of audit findings.

I. Assessing Internal Controls

When assessing the effectiveness of internal controls, entities should:

- i. Consider the significant risks and assess how they have been identified, evaluated and managed;
- ii. Assess the effectiveness of the related system of internal control in managing the significant risks, having regard, in particular, to any significant control weaknesses that have been reported;
- iii. Consider whether necessary actions are being taken promptly to remedy any significant control weaknesses; and
- iv. Consider whether the findings indicate a need for more extensive monitoring of the system of internal control.

There are five steps to assessing the effectiveness of internal controls based on the COSO internal control integrated framework 2013 including:

- i. Establish scope and accountability;
- ii. Identify and document risks and controls;
- iii. Evaluate effectiveness of controls;
- iv. Identify control gaps and deficiencies; develop corrective action plan(s); and
- v. Monitor and report the control gaps and corrective action plan (s) to management and/or governing body.

A compliance checklist should be developed to assist in conducting an annual control self - assessment. A sample is provided in *Appendix 1*.

II. Documentation Requirements

Documentation is a necessary part of an effective internal control system. The level and nature of documentation varies based on the size of the entity and the complexity of the operational processes the entity performs.

Management exercises judgment in determining the extent of documentation which is required to demonstrate the design, implementation, and operating effectiveness of an entity's internal control system. These guidelines include minimum documentation requirements as follows:

- i. If management determines that a principle is not relevant, then supports it with documentation that includes the rationale of how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively.
- ii. Management develops and maintains documentation of its internal control system.
- iii. Management documents in policies the internal control responsibilities of the organization.
- iv. Management evaluates and documents internal control weaknesses and determines appropriate corrective actions on a timely basis.

- v. Management evaluates and documents the results of ongoing monitoring and separate evaluations to establish the progress on implementation of corrective actions.

DRAFT

3.0. CHAPTER THREE: ROLES AND RESPONSIBILITIES FOR INTERNAL CONTROL

Internal control is primarily effected by an entity’s internal stakeholders including the governing body, management and all staff through their actions and communication. When the internal control activities are outsourced and effected by third parties, an entity’s management still bears ultimate responsibility for internal control systems. However, the actions of external stakeholders also impact the internal control system.

The “Three Lines Model” developed by the Institute of Internal Auditors provides a simple and effective way to help delegate and coordinate risk management roles and responsibilities and set role boundaries within the entity. These guidelines prescribe minimum roles and responsibilities, and entities should seek further clarification and direction from the National Treasury on application of this model especially when their structures do not allow the delegation of roles as prescribed below. Everyone in an organization has some responsibility for internal control:

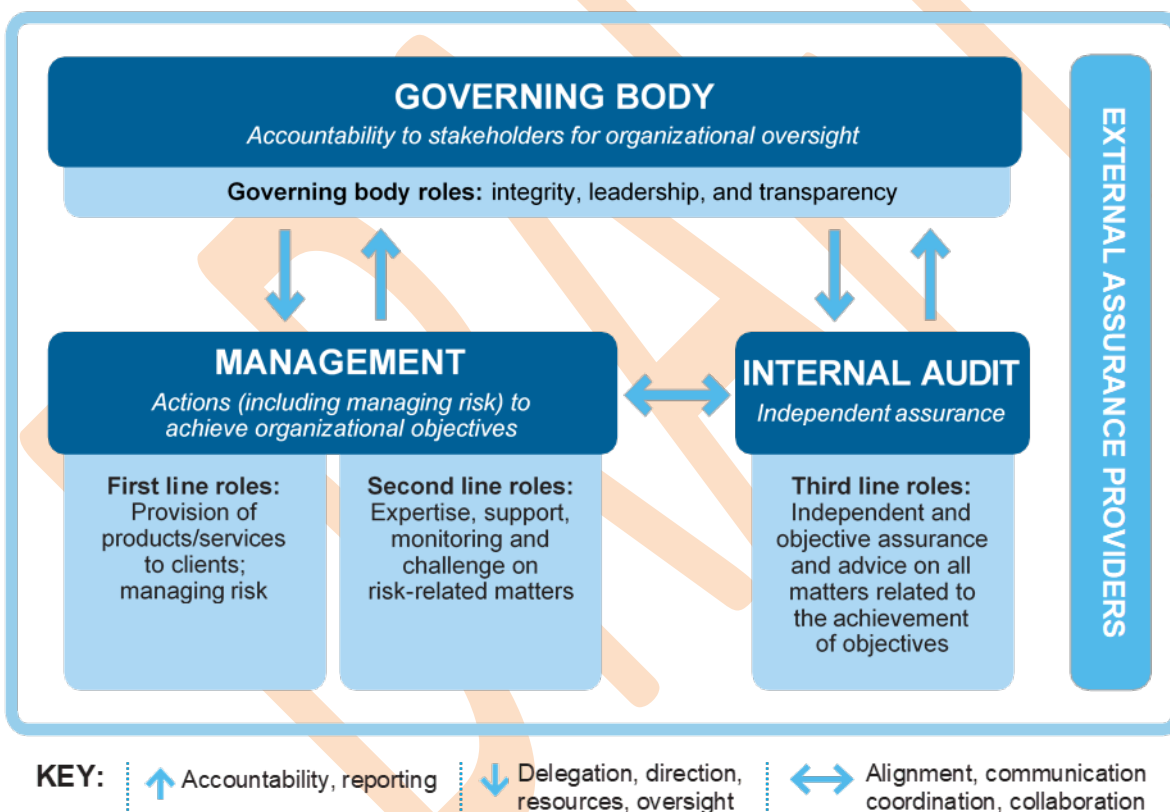


Figure 3 Three Lines Model (Source: The IIA, 2020)

3.1. The Governing body

The governing body (and its committees) plays an important role as it oversees and monitors management, approves policies and procedures, and sets the tone, along with management, for the entity to establish the importance of an adequate internal control system. The governing body

sets the expectation regarding an entity's integrity and ethical principles as well as transparency and accountability for the internal control performance. To oversee the internal control system, the governing body needs to establish adequate and open communication with other participants of the system including management and staff. To succeed in that role, the governing body needs to be capable, efficient, and objective. An effective governing body should understand the environment in which an entity operates, dedicate sufficient time to its duties, and be independent in its views and judgment. The governing body often executes certain responsibilities, including those related to internal controls, through its committees. The number, role, and composition of committees vary depending on legal and business requirements. The most common committees are audit, governance and risk which all contribute to the oversight of internal controls.

The governing body should:

- i. Establishes structures and processes for governance.
- ii. Oversight the establishment and maintenance of an effective and efficient system of internal control.
- iii. Set out its responsibility for internal controls in the Board Charter.
- iv. Delegate to management the responsibility of designing, implementing and monitoring effectiveness of internal control systems.
- v. Receive from the internal audit function a written assessment of the effectiveness of the system of internal controls on a quarterly basis.
- vi. Receive from the external auditor an assessment of the effectiveness of the system of internal control after the audit process.
- vii. Ensure that the internal audit function monitors for rectification, weaknesses noted by the external auditor.
- viii. Hold management to account on the effectiveness of the entity's system of internal control.

3.2. The Audit Committee

The audit committee which forms part of the Governing Body plays a key role in monitoring the effectiveness of internal control. Through interaction with management, internal and external assurance providers, the committee oversees the execution of control over the entity's corporate objectives. The PFM Regulations 2015 requires that the accounting officer of a National and County Government entity establishes an audit committee. Additionally, the audit committee guidelines Gazette Notice 2690 and 2691 requires that all public sector entities establish a audit committee to assist the governing body and management in maintaining an adequate system of internal controls. National Government Ministries, County Governments, Constitutional Commissions, and Independent Offices majority of the audit committee members are not part of the governing body. In State corporations and semi-Autonomous Government Agencies (SAGAs) audit committees are committees of the governing bodies.

The audit committee is responsible for playing a key role with respect to the integrity of the entity's financial and operational information, its system of governance, risk and internal controls, and the legal and ethical conduct of management and employees. The specific responsibilities include:

- i. Advising on the adequacy of the internal control framework and policies.
- ii. Evaluating whether processes are in place to address key roles and responsibilities in relation to risk management and the adequacy of the control environment to provide

- reasonable assurance that the systems of internal control are of a high standard and functioning as intended.
- iii. Reviewing the entity 's internal financial and operational controls (that is, the systems established to identify, assess, manage and monitor financial and operational risks).
 - iv. Receive reports from management on the effectiveness of the systems of internal control they have established and the reports of internal and external assurance providers.
 - v. Review and approve the statements included in the annual report in relation to internal control and the management of risk.
 - vi. Reporting to the governing body all major issues pertaining to the organization's controlling processes.

3.3. Management

Management is responsible for establishing an effective control environment in their entity. This is part of their stewardship responsibility over the use of public resources. Indeed, the tone managers set through their actions, policies, and communications can result in a culture of either positive or lax control. Planning, implementing, supervising, and monitoring are fundamental components of internal control. Management is ultimately accountable to the governing body.

To have an adequate and effective process for controlling operations, management have the following responsibilities.

3.3.1. Management Responsibilities in the First Line

First line roles are most directly aligned with the delivery of products and/or services to the public. This includes the roles of core and support functions. The key responsibilities are as listed below:

- i. Leads and directs actions (including managing risk) and application of resources to achieve the objectives of the organization.
- ii. Maintains a continuous dialogue with the governing body, and reports on: planned, actual, and expected outcomes linked to the objectives of the organization; and risk.
- iii. Establishes and maintains appropriate structures and processes for the management of operations and risk (including internal control).
- iv. Ensures compliance with legal, regulatory, and ethical expectations.
- v. Maintaining oversight and control over the risks facing the entity (e.g., directing all management and other staff to proactively identify risks to the system of internal control, considering the ever-increasing pace of change and networked interactions with stakeholders and resulting risk factors)
- vi. Guiding the development and performance of control activities at the entity level, and delegating to various levels of management the design, implementation, conduct, and assessment of internal control at different levels of the entity (e.g., processes and controls to be established)
- vii. Evaluating control deficiencies and the impact on the ongoing and long-term effectiveness of the system of internal control (e.g., meeting regularly with management from each department/functions to evaluate how they are carrying out their internal control responsibilities)
- viii. Execute corrective action plans as control exceptions or other issues arise.

3.3.2. Management Responsibilities in the Second Line

Second line roles provide assistance with managing risk and internal controls. Second line roles may be assigned to specialists to provide complementary expertise, support, monitoring, and challenge to those with first line roles. However, responsibility for managing risk remains a part of first line roles and within the scope of management. These will include but not limited to, risk officers, quality assurance officers, integrity officers, investigators, compliance officers and monitoring and evaluations officers. The key responsibilities are as listed below:

- i. Provides complementary expertise, support, monitoring, and challenge related to the management of risk and internal controls, including:
 - a. The development, implementation, and continuous improvement of risk management practices (including internal control) at a process, systems, and entity level.
 - b. The achievement of risk management objectives, such as: compliance with laws, regulations, and acceptable ethical behavior, internal control, information and technology security, sustainability, and quality assurance.
- ii. Provides analysis and reports on the adequacy and effectiveness of risk management (including internal control).
- iii. Guiding the development and implementation of internal control policies and procedures that address the objectives of their functional or operating function and verify that they are consistent with the entity-wide objectives.
- iv. Make recommendations on the controls, monitor their application within processes, and meet with management to report on the operation of controls.
- v. Establish an ongoing monitoring program to determine and report on the effectiveness with which the controlling processes accomplish their intended purpose.
- vi. Train and sensitize staff to maintain a level of competence to perform their duties.

3.4. Internal Audit Responsibilities in the Third Line

Internal audit provides independent and objective assurance and advice on the adequacy and effectiveness of governance, risk management and internal controls. It achieves this through the competent application of systematic and disciplined processes, expertise, and insight. It reports its findings to management and the governing body to promote and facilitate continuous improvement. In doing so, it may consider assurance from other internal and external providers.

The International Professional Practices Framework (IPPF) outlines that the internal audit activity must assist organizations in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement. That responsibility is carried out in the following steps:

- i. Ascertaining that the internal controls are adequately designed in relation to the related risk.
- ii. Determining that the internal controls are implemented and operating as intended in an effective and efficient manner.
- iii. The internal audit function includes evaluating the adequacy and effectiveness of controls in responding to risks within the entity's oversight, operations, and information systems regarding: Reliability and integrity of financial and operational information; Effectiveness and efficiency of operations and programs; Safeguarding of assets and Compliance with laws, rules, regulations, standards, policies, procedures, and contracts.
- iv. Reporting the results of audit work performed and offering recommendations for improving the internal control process to governing body and management.

- v. Coordinate audit activities with other assurance providers.
- vi. Monitoring implementation of recommendations.
- vii. Reports impairments to independence and objectivity to the governing body and implements safeguards as required.
- viii. Providing advisory on internal control framework design and implementation. This shall be done while putting the necessary safeguards. E.g training on controls

3.5. External Assurance Providers

External Assurance Providers in the public sector include but are not limited to, Office of the Auditor General, Regulators and Legislators (Oversight Committees). Their roles include:

- i. Satisfy legislative and regulatory expectations that serve to protect the interests of stakeholders.
- ii. Satisfy requests by management and the governing body to complement internal sources of assurance.

3.6. Other Stakeholders

These are other parties who have interest in the delivery of the entity's mandate. They include but not limited to, development partners, parent ministries, the National Treasury, Legislature, Judiciary and the general public. They contribute to the design of the internal controls and seek assurance that the internal controls are effective to safeguard the public interest.

Appendix 1: Annual Control Self-Assessment Compliance Checklist

Assessment Factor	Indication of Stronger Controls	Indication of Weaker Controls	Assessment					Recommended Actions
Strong - Weak			1	2	3	4	5	
Section 1 – Control Environment								
1 - Integrity and Ethical Values								
1.1 Acceptable business practices.	Department management (faculty and supervisory staff) understand the Entity's policies covering matters such as legitimate use of Entity resources.	Policies are poorly understood						
1.2 Codes of conduct.	Department management understands the Entity's policies governing relationships with sponsors, suppliers, creditors, regulators, the community, and the public at large.	Policies are poorly understood.						
1.3 Conflicts of interests.	Department management understands the Entity's policies regarding potential conflicts of interest.	Policies are poorly understood.						
1.4 Integrity.	Department management sets a good example and regularly communicates high expectations regarding integrity and ethical values.	Management does not set a good example and/or does not communicate high expectations regarding integrity and ethical values.						
2 – Commitment to Competence								
2.1 Job descriptions.	Responsibilities are clearly defined in writing and communicated as appropriate.	Responsibilities are poorly defined or poorly communicated.						

2.2 Knowledge and Skills.	Department management (faculty and supervisory staff) understand the knowledge and skills required to accomplish tasks.	Management does not adequately consider knowledge and skill requirements.						
---------------------------	---	---	--	--	--	--	--	--

DRAFT

Assessment Factor	Indication of Stronger Controls	Indication of Weaker Controls	Assessment					Recommended Actions
			1	2	3	4	5	
Strong - Weak								
2.3 Employee competence.	Department management is aware of competency levels, and is involved in training and increased supervision when competency is low.	Management is not adequately aware of competency levels, or does not actively address problems.						
3 – Management’s Philosophy and Operating Style								
3.1 Communication	Department management engages in open disclosure of financial or business issues with appropriate Entity personnel.	Management is secretive and reluctant to conduct business or deal with issues in an open manner.						
3.2 Laws and regulations.	There is active concern and effort to ensure compliance with the letter and intent of laws and regulations.	Management is willing to risk the consequences of noncompliance.						
3.3 Getting the job done.	Management is concerned with and exerts effort to get the job done right the first time.	Management is willing to get the job done without adequate regard to quality.						
3.4 Exceptions to policy.	Exceptions to policy are infrequent. When they occur they must be approved and well documented.	Exceptions to policy are the norm and are rarely documented.						
3.5 Approach to financial accountability.	Management’s approach shows concern and appreciation for accurate and timely reporting. Budgeting and other financial estimates are generally conservative.	Financial accountability is given low priority.						
3.6 Emphasis on meeting budget and other financial and operating goals.	Realistic budgets are established and results are actively monitored. Corrective action is taken as necessary.	Management either shows little concern (climate of laxness), or makes						

		unreasonable (climate of fear).	demands						
--	--	------------------------------------	---------	--	--	--	--	--	--

DRAFT

Assessment Factor	Indication of Stronger Controls	Indication of Weaker Controls	Assessment					Recommended Actions
			1	2	3	4	5	
Strong - Weak								
3.7 Approach to decision making.	Decision-making processes are deliberate and consistent. Decisions are made after careful consideration of relevant facts. Policies and procedures are in place to ensure appropriate levels of management are involved.	Decision making is nearly always informal. Management makes arbitrary decisions with inadequate discussion and analysis of the facts.						
4 – Organizational Structure								
4.1 Complexity of the organizational structure.	Complexity of the structure is commensurate with the organization. Lines of reporting are clear and documentation is up-to-date.	Lines of responsibility are unclear or unnecessarily complicated for the size and activities of the entity.						
4.2 Organization charts.	Documentation exists and is up to date.	Documentation does not exist or is out-of-date. The documented structure does not correspond with actual responsibilities.						
4.3 Size of the management group.	Size is commensurate with the complexity of the department and its growth.	Size is not appropriate (e.g., too many levels, too dispersed, or too "thin").						
4.4 Stability of the management group.	Low turnover.	High turnover.						
5 – Assignment of Authority and Responsibility								
5.1 Delegation of authority and assignment of responsibility for operating and financial functions.	Delegation of authority and assignment of responsibility is clearly defined. Individuals are held accountable for results.	Decisions are dominated by one or a few individuals. Roles and responsibilities of middle management are unclear.						
5.2 Authority limits.	Authority limits are clearly defined in writing and communicated as appropriate.	Policies and procedures covering authority limits are informal or poorly communicated.						

5.3 Delegated signature authority.	Appropriate limits have been placed on each delegation of signature authority. Management reviews and updates signature records as turnover occurs.	Signature authority is delegated without adequate consideration. Delegated authority is not in line with employee knowledge, training, or competence.							
5.4 Knowledge and experience.	Key personnel are knowledgeable and experienced. Management does not delegate authority to inexperienced individuals.	Key personnel are inexperienced. Management delegates authority without regard to knowledge and experience.							

DRAFT

Assessment Factor	Indication of Stronger Controls	Indication of Weaker Controls	Assessment					Recommended Actions
			1	2	3	4	5	
Strong - Weak								
5.5 Resources.	Management provides the resources needed foremployees to carry out their duties.	Management does not provide necessary resources.						
6 – Human Resource Policies and Practices								
6.1 Selection of personnel.	A careful hiring process is in place. The Human Resources Department is involved in identifying potential employees based on job requirements.	The hiring process is informal, and sometimesproceeds without adequate involvement by higher-level supervisors.						
6.2 Training.	On-the-job and other training programs have defined objectives. They are effective and important.	Training programs are inconsistent, ineffective, or are given low priority.						
6.3 Supervision policies.	Personnel are adequately supervised. They have a regular resource for resolving problems.	Regular supervision does not exist or is ineffective. Employees are frustrated and feelthey ‘have nowhere to go’ with issues.						
6.4 Inappropriate behavior.	Inappropriate behavior is consistently reprimanded in a timely and direct manner, regardless of the individual's position or status.	Reprimands are not timely, direct, or are notconsistently applied (climate of favoritism).						
6.5 Evaluation of personnel.	An organized evaluation process exists.	The evaluation process is ad hoc and inconsistent. Performance issues are notformally addressed.						
6.6 Methods to compensate personnel.	Compensation decisions are based on a formal process with meaningful involvement of morethan one level of management. The effect of performance evaluations on compensation decisions is defined and communicated.	Compensation decisions are ad hoc, inconsistent, or inadequately reviewed by management.						

6.7 Staffing of critical functions.	Critical functions are adequately staffed, with reasonable workloads.	There is inadequate staffing and frequent periods of overwork and "organizational stress."						
6.8 Turnover. Particularly turnover in financially responsible positions.	Low turnover. Management understands root causes of turnover.	High turnover. Management does not understand root causes.						

DRAFT

Assessment Factor	Indication of Stronger Controls	Indication of Weaker Controls	Assessment					Recommended Actions
			1	2	3	4	5	
Strong - Weak								
Section 2 – Risk Assessment								
7 – Organizational Goals and Objectives								
7.1 Unit-wide objectives.	A formal mission or value statement is established and communicated throughout the department.	A unit-wide mission or value statement does not exist.						
7.2 Critical success factors.	Factors that are critical to achievement of department-wide objectives are identified. Resources are appropriately allocated between critical success factors and objectives of lesser importance.	Success factors are not identified or prioritized.						
7.3 Activity-level objectives.	Realistic objectives are established for all key activities including operations, financial reporting and compliance considerations.	Activity-level objectives do not exist.						
7.4 Measurement of objectives.	Department-wide and activity level objectives include measurement criteria and are periodically evaluated.	Performance regarding objectives is not measured. Targets are not set.						
7.5 Employee involvement.	Employees at all levels are represented in establishing the objectives.	Management dictates objectives without adequate employee involvement.						
7.6 Long and short-range planning.	Long and short-range plans are developed and are written. Changes in direction are made only after sufficient study is performed.	No organized planning process exists. There are frequent shifts in direction or emphasis.						
7.7 Budgeting system.	Detailed budgets are developed by area of responsibility following prescribed procedures and realistic expectations. Plans and budgets support achievement of department-wide	Budgets do not exist or are "backed into" depending on desired outcome.						

	action steps.								
7.8 Strategic planning for information systems.	Planning for future needs is done well in advance of expected needs and considers various scenarios.	The information system lags significantly behind the needs of the business.							

DRAFT

Assessment Factor	Indication of Stronger Controls	Indication of Weaker Controls	Assessment					Recommended Action
			1	2	3	4	5	
Strong - Weak								
8 – Risk Identification and Prioritization								
8.1 Identification and consideration of external risk factors.	A process exists to identify and consider the implications of external risk factors (economic changes, changing sponsor, student and community needs or expectations, new or changed legislation or regulations, technological developments, etc.) on department-wide objectives and plans.	Potential or actual external risk factors are not effectively identified or evaluated.						
8.2 Identification and consideration of internal risk factors.	A process exists to identify and consider the implications of internal risk factors (new personnel, new information systems, changes in management responsibilities, new or changed educational or research programs, etc.) on department-wide objectives and plans.	Potential or actual internal risk factors are not effectively identified or evaluated.						
8.3 Prioritization of risks.	The likelihood of occurrence and potential impact (monetary and otherwise) have been evaluated. Risks have been categorized as tolerable or requiring action.	Risks have not been prioritized.						
8.4 Approach to studying risks.	In-depth, cost / benefit studies are performed before committing significant unit resources.	Risks are accepted with little or no study.						
8.5 Process for monitoring risks.	A risk management program is in place to monitor and help mitigate exposures.	Exposure is dealt with on a case by case basis. Regular efforts or programs to manage risks do not exist.						
8.6 Consultation with external advisors.	External advisors are consulted as needed to supplement internal expertise.	Internal expertise regarding risk and control issues is inadequate. Assistance is						

		never sought from outside sources.							
9 – Managing Change									
9.1 Commitment to change.	Management promotes continuous improvement and solicits input and feedback on the implications of significant change.	Management promotes the status quo, even when changes are needed to meet important business needs.							

DRAFT

Assessment Factor	Indication of Stronger Controls	Indication of Weaker Controls	Assessment					Recommended Action
			1	2	3	4	5	
Strong - Weak								
9.2 Support of change.	Management is willing to commit resources to achieve positive change.	Management offers no resources to facilitate change.						
9.3 Routine change.	Mechanisms exist to identify, prioritize, and react to routine events (i.e., turnover) that affect achievement of unit-wide objectives or action steps.	Procedures are not present or are ineffective.						
9.4 Economic change.	Mechanisms exist to identify and react to economic changes.	Procedures are not present or are ineffective.						
9.5 Regulatory change.	Mechanisms exist to identify and react to regulatory changes (maintain membership in associations that monitor laws and regulations, participate in Entity forums, etc.).	Procedures are not present or are ineffective.						
9.6 Technological change.	Mechanisms exist to identify and react to technological changes and changes in the functional requirements of the unit.	Procedures are not present or are ineffective.						
Section 3 – Control Activities								
10 – Written Policies and Procedures								
10.1 Entity's policies and procedures.	The entity has formulated applicable policies and procedures that apply to the department.	Knowledge of Entity policy and procedures are not well known in the department.						
10.2 Department policies and procedures.	The department has documented its own policies and procedures if applicable. They are well understood by department employees.	Department policies and procedures are not well known or documented.						
11 – Control Procedures								

11.1 Senior management Entity's reviews.	Senior management monitors the department's performance against objectives and budget.	Senior management does not monitor department performance.						
--	--	--	--	--	--	--	--	--

DRAFT

Assessment Factor	Indication of Stronger Controls	Indication of Weaker Controls	Assessment					Recommended Action
			1	2	3	4	5	
Strong - Weak								
11.2 Objective performance reviews by department management of major initiatives.	Reviews are made of actual performance compared to objectives and previous periods for all major initiatives. Management analyzes and follows up as needed.	Analyses are not performed or management does not follow up on significant deviations.						
11.3 Financial performance reviews by department management.	Reviews are made of actual performance versus budgets, forecasts, and performance in prior periods for all major initiatives. Management analyzes and follows up as needed.	Analyses are not performed or management does not follow up on significant deviations.						
11.4 Direct functional or activity management by department management.	Performance reviews are made of specific functions or activities, focusing on compliance, financial or operational issues.	No performance reviews occur.						
11.5 Performance indicators.	Unexpected operating results or unusual trends are investigated.	Operating results and trends are not monitored.						
11.6 Financial transactions, timekeeping records and reconciliations.	Financial transactions, timekeeping and reconciliations are completed timely. Management performs a diligent review and approval by signature and date or electronically.	The activities are not performed timely or regularly. Management does not carefully review or formally approve.						
11.7 Sponsored project account management.	Sponsored project accounts are reviewed and reconciled. PIs certify the expenditures timely. Department management monitors the portfolio of sponsored accounts for compliance and fiscal responsibility.	Sponsored project accounts are not monitored; reconciliations and certifications are not timely.						

11.8 Use of restricted funds (gifts).	Restrictions on use are well documented, and are understood by employees who administer the funds. Usage is monitored by management, accounts are reconciled.	Restrictions are not clearly documented. Restricted fund accounts are not monitored; usage may not match restrictions.						
---------------------------------------	---	--	--	--	--	--	--	--

DRAFT

Assessment Factor	Indication of Stronger Controls	Indication of Weaker Controls	Assessment					Recommended Action
			1	2	3	4	5	
Strong - Weak								
11.9 Information processing.	Controls exist to monitor the accuracy and completeness of information as well as authorization of transactions.	No information processing controls are in place.						
11.10 Physical controls.	Equipment, supplies, inventory, cash and other assets are physically secured and periodically counted and compared to the amounts shown on control records. (if applicable)	Equipment, supplies, inventory, cash and other assets are not protected. Control records do not exist or are not up to date.						
11.11 Training and guidance for asset custodians.	Adequate guidance and training are provided to personnel responsible for cash or similar assets.	No training or guidance is provided.						
11.12 Separation of duties.	Financial duties are divided among different people (responsibilities for authorizing transactions, recording them and handling the asset are separated).	No significant separation of financial duties among different employees.						
11.13 Record retention.	Unit employees understand which records they are responsible to maintain and the required retention period. Records are appropriately filed.	Unit employees do not understand which records they are responsible for maintaining. The filing system is inadequate.						
11.14 Disaster response plan.	A disaster response and recovery plan has been developed and is understood by key personnel.	No disaster response or recovery plan exists.						
12 – Controls over Information Systems								

12.1 Local information systems and LANs.	System operations are documented; software is appropriately acquired and maintained; access to the system, programs and data is controlled; the system is maintained in a secure environment; applications are appropriately developed and maintained.	Inadequate controls over local informationsystems or LANs.						
--	--	--	--	--	--	--	--	--

DRAFT

Assessment Factor	Indication of Stronger Controls	Indication of Weaker Controls	Assessment					Recommended Actions
Strong - Weak								
			1	2	3	4	5	
12.2 Application controls.	The department controls its computer applications by diligent and timely response to edit lists, rejected transactions and other control and balancing reports. Controls ensure a high level of data integrity including completeness, accuracy, and validity of all information in the system.	Application controls are not used.						
12.3 Back Up.	Key data and programs on LANs or desktop computers are appropriately backed up and maintained. Off-site storage is adequate considering possible risks of loss.	No formal back up procedures exist. Management has not informed staff of back up requirements.						

Assessment Factor	Indication of Stronger Controls	Indication of Weaker Controls	Assessment					Recommended Actions
Strong - Weak			1	2	3	4	5	
Section 4 – Information and Communication								
13 – Access to Information								
13.1 Relevant external information.	Department members receive relevant information regarding legislation, regulatory developments, economic changes or other external factors that affect the department.	Relevant information is not available.						
13.2 Management reporting system.	An executive information system exists. Information and reports are provided timely. Report detail is appropriate for the level of management. Data is summarized to facilitate decision making.	A formal reporting system does not exist. Reports are not timely or are not at appropriate levels of detail.						
13.3 Management of information security.	Information is evaluated and classified based on level of integrity, confidentiality and availability. Individuals with access to information are trained to understand their responsibilities related to the information.	Information used by the unit has not been evaluated and classified. Employees are not trained with respect to information security.						
14 – Communication Patterns								
14.1 Trust.	Management promotes and fosters trust between employees, supervisors and others within the Department.	Interactions among faculty, staff and/or with other units is characterized by low levels of trust.						
14.2 Policy enforcement and discipline.	Employees who violate an important policy are disciplined. Management's communications and actions are consistent with policies.	Violations, while not condoned officially, are often overlooked. Management's actions are inconsistent with official policies.						

14.3 Recommendations for improvement.	Employees are encouraged to provide recommendations for improvement. Ideas are recognized and rewarded.	Employees' ideas are not welcomed.						
---------------------------------------	---	------------------------------------	--	--	--	--	--	--

DRAFT

Assessment Factor	Indication of Stronger Controls	Indication of Weaker Controls	Assessment					Recommended Actions
Strong - Weak								
			1	2	3	4	5	
14.4 Formal communications.	Formal methods are used to communicate unit policies and procedures (e.g., manuals, training programs, written codes of conduct, and acceptable business practices).	To the extent that they exist, policies are buried in unused manuals and documents.						
14.5 External communications.	Standards and expectations are communicated to key outside groups or individuals (e.g., vendors, consultants, donors, sponsors, subcontractors, sub-recipients).	No external communication of standards and expectations.						
14.6 Informal communications.	Employees are kept informed of important matters (downward communication) and are able to communicate problems to persons with authority (upward communication). There is effective functional coordination within the department (lateral communication).	Most information is received by the "grapevine."						
14.7 Communication with evaluators.	Information is openly shared with outside evaluators.	Information is kept secret from outside evaluators.						
Section 5 – Monitoring								
15 – Management Supervision								
15.1 Effectiveness of key control activities.	Management routinely spot-checks transactions, records and reconciliations to ensure expectations are met.	Management never performs spot-checks.						
15.2 Management supervision of financial and timekeeping activities.	Knowledge of Entity financial and timekeeping policies are known by those with those responsibilities in the department.	Policies are ad hoc or poorly communicated.						

15.3 Management supervision of new systems development.	Policies are defined for developing new systems or changes to existing systems (cost/benefit analysis, team composition, user specifications, documentation, acceptance testing, and user approval).	Policies and procedures are ad hoc, poorly communicated, or ineffective.							
---	--	--	--	--	--	--	--	--	--

DRAFT

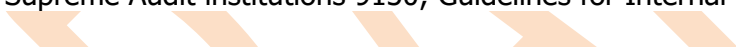

Assessment Factor	Indication of Stronger Controls	Indication of Weaker Controls	Assessment					Recommended Actions
			1	2	3	4	5	
Strong - Weak								
15.4 Budget analysis.	Budgets are compared to actual results and deviations are followed up on a timely basis. Adequate consideration is given to commitments.	An analysis of actual versus budgeted results is not performed, or management does not follow up on deviations.						
16 – Outside Sources								
16.1 Industry and professional associations.	Data is used to compare the unit's performance with peers or industry standards.	Comparative data is not regularly monitored.						
16.2 Regulatory authorities.	Reports from regulatory bodies are considered for their internal control implications.	Response is limited to what is necessary to "get by" the regulators.						
16.3 Sponsors, students, suppliers, creditors, and other third parties.	Root causes of inquiries or complaints are investigated and considered for internal control implications.	Inquiries or complaints are dealt with case-by-case, with little or no follow-up.						
16.4 External auditors.	Information provided by external auditors about control-related matters are considered and acted on.	Findings are referred to lower levels or are explained away.						
17 – Response Mechanisms								
17.1 Management follow-up of violations of policies.	Timely corrective action is taken.	Follow-up is sporadic.						
17.2 External or internal audit reports.	Audit report issues are considered and immediately acted upon at appropriate levels.	Consideration of issues from audit reports are delegated to lower levels or is given low priority.						
17.3 Changes in conditions (e.g., economic, regulatory, technological, or competitive).	Changes are anticipated and routinely integrated into ongoing long- and short-range planning.	Responses are reactive rather than proactive.						

DRAFT

Assessment Factor	Indication of Stronger Controls	Indication of Weaker Controls	Assessment					Recommended Actions
			1	2	3	4	5	
Strong - Weak								
18.1 Monitoring of control environment.	Management periodically assesses employee attitudes, reviews the effectiveness of the organization structure, and evaluates the appropriateness of policies and procedures.	Assessment processes do not exist.						
18.2 Evaluation of risk assessment process.	Management periodically evaluates the effectiveness of its risk assessment process.	Assessment processes do not exist.						
18.3 Assessment of design and effectiveness of internal controls.	Internal controls are subject to a formal and continuous internal assessment process.	Assessment processes do not exist.						
18.4 Evaluation of information and communication systems.	Management periodically evaluates the accuracy, timeliness and relevance of its information and communication systems. Management questions information on management reports that appears unusual or inconsistent.	Assessment process does not exist.						

Appendix 2: References



- i. The Constitution of Kenya, 2010
 - ii. The PFM Act, 2012
 - iii. The PFM Regulations 2015
 - iv. COSO Internal Control – Integrated Framework, 2013.
 - v. International Professional Practice Framework.
 - vi. COBIT 2019: Control Objectives for Information and Related Technology (Information Systems Audit and Control Association's IT Governance framework)
 - vii. The Standards for Internal Control in the Federal Government; The Green Book US.
 - viii. The Criteria for Control (CoCo) Framework.
 - ix. International Organization of Supreme Audit Institutions 9100 Guidelines for Internal Control Standards for the Public Sector.
 - x. International Organization of Supreme Audit Institutions 9110; Guidance for reporting for effectiveness of internal controls.
 - xi. International Organization of Supreme Audit Institutions 9120; Internal Control- Providing a foundation for accountability in government.
 - xii. International Organization of Supreme Audit institutions 9130; Guidelines for Internal Control Standards for the Public Sector.
- 
- 

Appendix 3: Glossary of Terms

GLOSSARY OF TERMS		
1.	Access control	In information technology, controls designed to protect resources from unauthorized modification, loss, or disclosure.
2.	Accountability	The process whereby public service bodies and the individuals within them are held responsible for their decisions and actions, including their stewardship of public funds and all aspects of performance.
3.	Application	Computer program designed to help people perform a certain type of work, including specific functions, such as payroll, inventory control, accounting, and mission support. Depending on the work for which it is designed, an application can manipulate text, numbers, graphics, or a combination of these elements.
4.	Application controls	The structure, policies, and procedures that apply to separate, individual application systems and are designed to cover the processing of data within specific applications software.
5.	Audit	Review of a body's activities and operations to ensure that these are being performed or are functioning in accordance with objectives, budget, rules and standards. The aim of this review is to identify, at regular intervals, deviations which might require corrective action.
6.	Audit committee	A committee of the Governing body whose role typically focuses on aspects of financial reporting and on the entity's processes to manage business and financial risk, and for compliance with significant applicable legal, ethical, and regulatory requirements.
7.	Budget	Quantitative, financial expression of a program of measures planned for a given period. The budget is drawn up with a view to planning future operations and to making ex post facto checks on the results obtained.
8.	Budgetary control	Control by which an authority which has granted an entity a budget ensures that this budget has been implemented in accordance with the estimates, authorizations and regulations.
9.	Collusion	A cooperative effort among employees to defraud a business of cash, inventory, or other assets.
10.	Compliance	Having to do with conforming with laws and regulations applicable to an entity. Conformity and adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.
11.	Component of internal control	One of five elements of internal control. The internal control components are the entity's internal control environment, risk assessment, control activities, information and communication, and monitoring. (COSO 2013).
12.	Control	Defined as action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. (CIAS, 2024).
13.	Control activity	Control activities are the policies and procedures established to address risks and to achieve the entity's objectives. The procedures that an organization puts in place to treat risk are called internal control activities.
14.	COSO	Committee of Sponsoring Organizations of the Treadway Commission. In May 2013, it published the Internal Control – Integrated Framework.

15.	Data	Facts that can be communicated and manipulated.
16.	Deficiency	A perceived, potential or real internal control shortcoming or an opportunity to strengthen internal control to provide a greater likelihood that the entity's objectives are achieved. (COSO 2013)
17.	Design	1. Intent. As used in the definition, internal control is intended to provide reasonable assurance as to the achievement of objectives; when the intent is realized, the system can be deemed effective. 2. Plan; the way a system is supposed to work, contrasted with how it actually works. (COSO 2013)
18.	Detective control	A control designed to discover an unintended event or result (contrast with preventive control) (COSO 2013)
19.	Documentation	Documentation of the internal control structure is the material and written evidence of the components of the internal control process, including the identification of an organizations' structure and policies and its operating categories, its related objectives and control activities. These should appear in documents such as management directives, administrative policies, procedures manuals, and accounting manuals.
20.	Economical	Not wasteful or extravagant. It means getting the right amount of resources, of the right quality, delivered at the right time and place, at the lowest cost.
21.	Effectiveness	The extent to which objectives are achieved and the relationship between the intended impact and the actual impact of an activity.
22.	Efficient	Refers to the relationship between the resources used and the outputs produced to achieve the objectives. It means that minimum resource inputs are used to achieve a given quantity and quality of output, or a maximum output with a given quantity and quality of resource inputs.
23.	Entity	An organization of any size established for a particular purpose. An entity, for example, may be a business enterprise, not-for-profit organization, government body or academic institution. Other terms used as synonyms include organization and department.
24.	Ethical	Relates to moral principles. Ethical values, moral values that enable a decision maker to determine an appropriate course of behavior; these values should be based on what is "right," which may go beyond what is legally required.
25.	External audit	Audit carried out by a body which is external to and independent of the audit client, the purpose being to give an opinion on and report on the accounts and the financial statements, the regularity and legality of operations, and/or the financial management.
26.	Fraud	An unlawful interaction between two entities, where one party intentionally deceives the other through the means of false representation in order to gain illicit, unjust advantage.
27.	Internal control	Internal control is an integral process that is effected by an entity's management and personnel and is designed to address risks and provide reasonable assurance that in pursuit of the entity's mission, the following general objectives are being achieved: executing orderly, ethical, economical, efficient and effective operations.
28.	Management intervention	Management's actions to overrule prescribed policies or procedures for legitimate purposes; management intervention is usually necessary to deal

		with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately by the system (contrast this term with Management Override).
29.	Management override	Management's overruling of prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's financial condition or compliance status (contrast this term with Management Intervention).
30.	Management process	The series of actions taken by management to run an entity. Internal control is a part of and integrated with the management process.
31.	Manual controls	Controls performed manually, not by computer (contrast with Computer Controls).
32.	Monitoring	Monitoring is a component of internal control and it is the process that assesses the quality of the internal control system's performance over time.
33.	Objectivity	An unbiased mental attitude that allows internal and external auditors to perform engagements in such a manner that they have an honest belief in their work product and that no significant quality compromises are made. Objectivity requires the auditors not to subordinate their judgment on audit matters to that of others.
34.	Operations	Used with "objectives" or "controls": having to do with the effectiveness and efficiency of an entity's activities, including performance.
35.	Policy	Management's dictate of what should be done to effect control. A policy serves as the basis for procedures for its implementation.
36.	Preventive control	A control designed to avoid unintended events or results (contrast with detective control).
37.	Procedure	An action that implements a policy.
38.	Processing	In information technology, the execution of program instructions by the computer's central processing unit.
39.	Public accountability	The obligations of persons or entities, including public enterprises and corporations, entrusted with public resources to be answerable for the fiscal, managerial and program responsibilities that have been conferred on them, and to report to those that have conferred these responsibilities on them
40.	Public sector	The term 'public sector' refers to national governments, County governments, and related governmental entities (for example, agencies, boards, State Corporations, Semi-autonomous Government Agencies, commissions, Independent offices and government enterprises).
41.	Reasonable assurance	Equates to a satisfactory level of confidence under given considerations of costs, benefits, and risks.
42.	Residual risk	The risk that remains after management responds to the risk.
43.	Risk	The possibility that an event will occur and adversely affect the achievement of objectives.
44.	Risk appetite	The amount of risk to which the entity is prepared to be exposed before it judges action to be necessary.
45.	Risk assessment	Risk assessment is the process of identifying and analyzing relevant risks to the achievement of the entity's objectives and determining the appropriate response.

46.	Risk assessment cycle	An ongoing, iterative process to identify and analyze altered conditions, opportunities and risks and to take actions as necessary, in particular modifying internal control to address changing risk.
47.	Risk evaluation	Means estimating the significance of a risk and assessing the likelihood of the risk occurrence.
48.	Risk profile	An overview or matrix of the key risks facing an entity or sub-unit that includes the level of impact (e.g., high, medium, low) along with the probability or likelihood of the event occurring.
49.	Risk tolerance	The acceptable variation relative to the achievement of objectives. (COSO ERM)
50.	Segregation (or separation) of duties	To reduce the risk of error, waste, or wrongful acts and the risk of not detecting such problems, no singular individual or team should control all key stages (authorizing, processing, recording, reviewing) of a transaction or event.
51.	Stakeholders	Parties that are affected by the entity, such as shareholders, the communities in which the entity operates, employees, customers and suppliers. (COSO ERM)
52.	Uncertainty	Inability to know in advance the exact likelihood or impact of future events. (COSO ERM)
53.	Value for money	Achieve Economy, Effectiveness and Efficiency