THE ANNUAL INTERNAL AUDIT, RISK & FORENSIC CONFERENCE

Venue: Sarova Whitesands, Mombasa

Date: 10th December 2020

Presenter: CPA Phares Chege

Deputy Commissioner, Internal Audit, KRA

About CPA Phares Chege

Profession

- Audit & Risk management practitioner for over 16 years
- Experience in public Sector – 70% of working life
- Experience in private Sector – 30% of working life

Some of the Organizations worked with:

- Kenya Revenue Authority
- Siginon Group Limited
- Higher Education Loans Board
- KPMG East Africa
- KeNHA
- Office of the auditor General

Qualifications

- MBA (Accounting)
- BA (Economics)
- Certified Public Accountant of Kenya
- Certified Internal Audit Quality Assessor
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Operational Risk Practitioner (CORP)

Training experience

Since 2004 with focus on:

- Internal Auditing & QAIP
- Enterprise Risk Management
- Forensic Audits
- Data Analytics
- Strategic Management
- Financial Reporting

CONTENT

1	Discussion of the relevant audit governance documents: Audit Charters, IA strategic plan, SOPs and Annual Workplan	45 MINUTES
2	Deep dive into typical substantive audit procedures for key processes in the public & private sector audit: Developing audit programs	45 MINUTES
3	Questions and discussions	30 MINUTES

CLOSE

1. Internal Audit Governance Documents

1. Internal Audit Governance Documents – Key Documents - External

1. Internal Audit Governance Documents – IPPF

1. Internal Audit Governance Documents – PFM Act

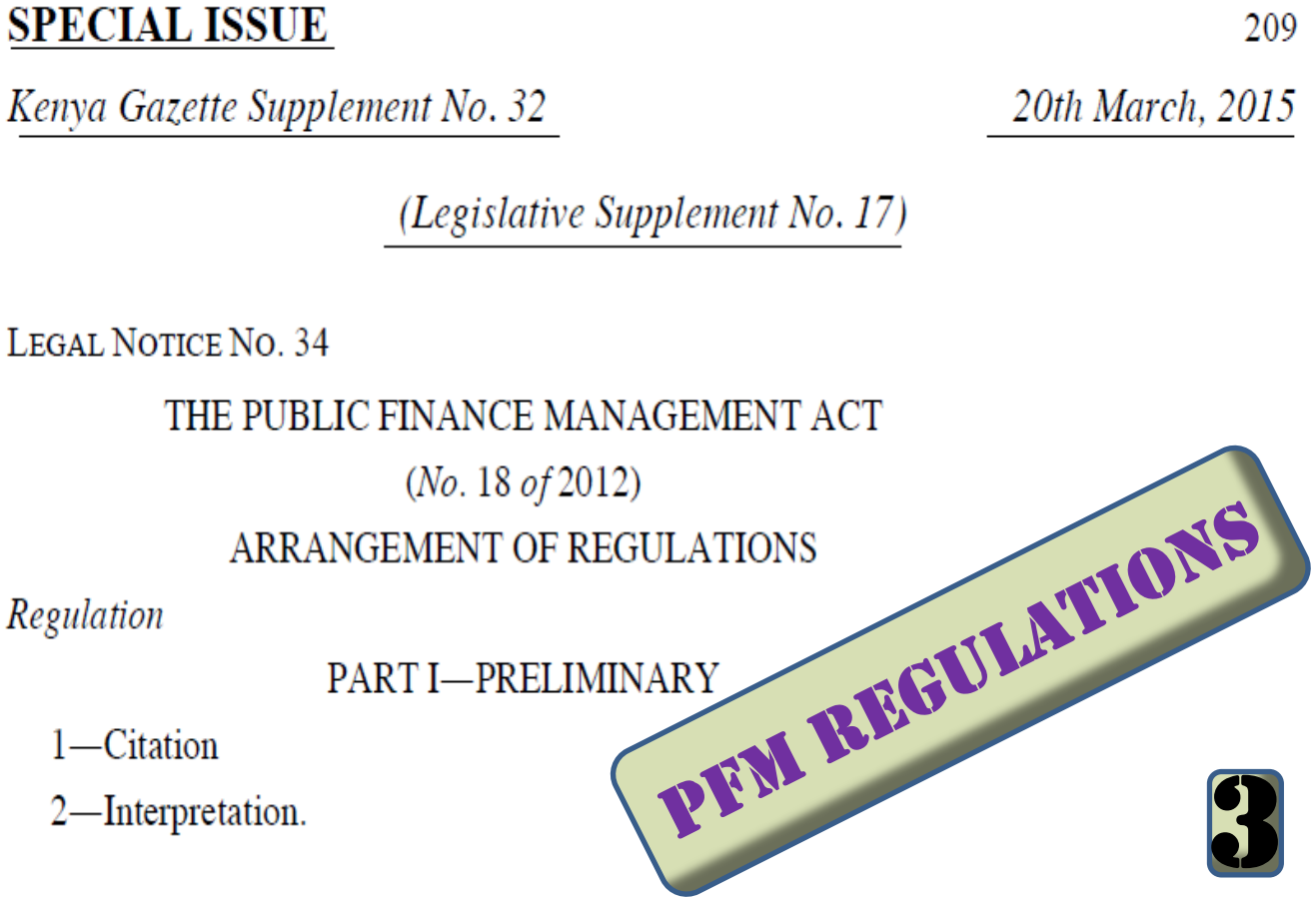
Internal Audit function Sec 73 and 155

1a) Every national/ county government entity shall ensure has appropriate arrangements in place for conducting **internal audit** according to the guidelines of the Accounting Standards Board

2) Regulations may prescribe requirements to be complied with in conducting internal audits.

5) Every government public entity shall establish an **audit committee** whose composition and functions shall be as prescribed by the regulations.

1. Internal Audit Governance Documents – PFM Regulations



SPECIAL ISSUE 209

Kenya Gazette Supplement No. 32 *20th March, 2015*

(Legislative Supplement No. 17)

LEGAL NOTICE NO. 34

THE PUBLIC FINANCE MANAGEMENT ACT

(*No.* 18 *of* 2012)

ARRANGEMENT OF REGULATIONS

Regulation

PART I—PRELIMINARY

1—Citation

2—Interpretation.

National government entities

Regulation 160-182

County government entities

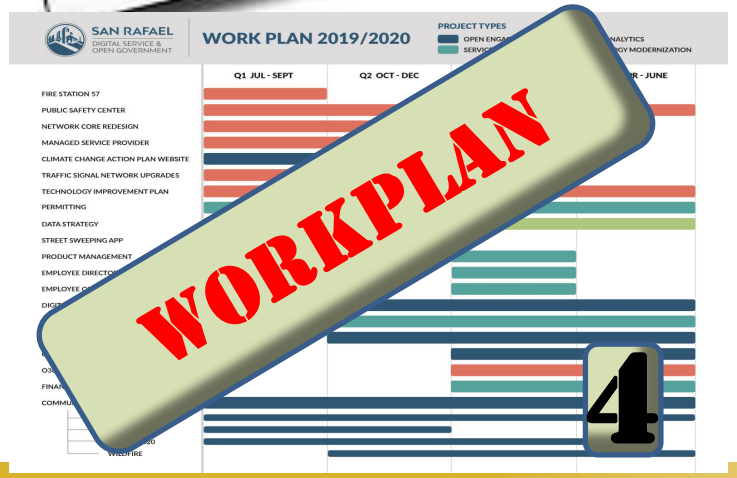
Regulation 153-175

1. Internal Audit Governance Documents – Key Documents - Internal

1

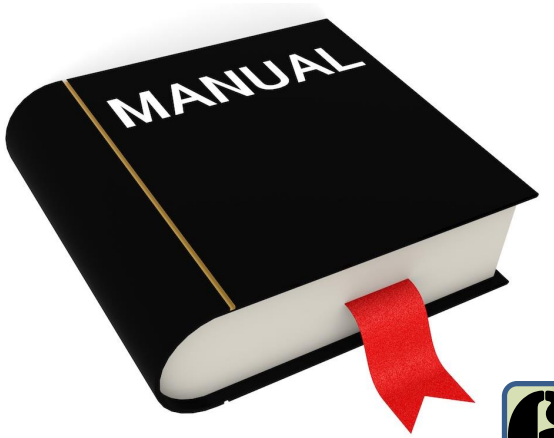
2

3



4

5



6

Vision: A world class Professional A

1. Internal Audit Governance Documents – Policies

Policies

1. Internal Audit Charter
2. Audit Committee charter [sometimes combined with Risk]
3. Risk Management policy

1. Internal Audit Governance Documents –Strategic Plan

Standard 2000 – Managing the Internal Audit Activity

The internal audit activity adds value to the organization and its stakeholders when it considers **strategies, objectives,** and **risks;** strives to offer ways to enhance governance, risk management and control processes; and objectively provides relevant assurance.

1. Internal Audit Governance Documents –SOPs

Standard 2040 – Policies and Procedures

CAE must establish policies and **procedures** to guide the internal audit activity.

Procedures are step by step guides on internal audit processes.

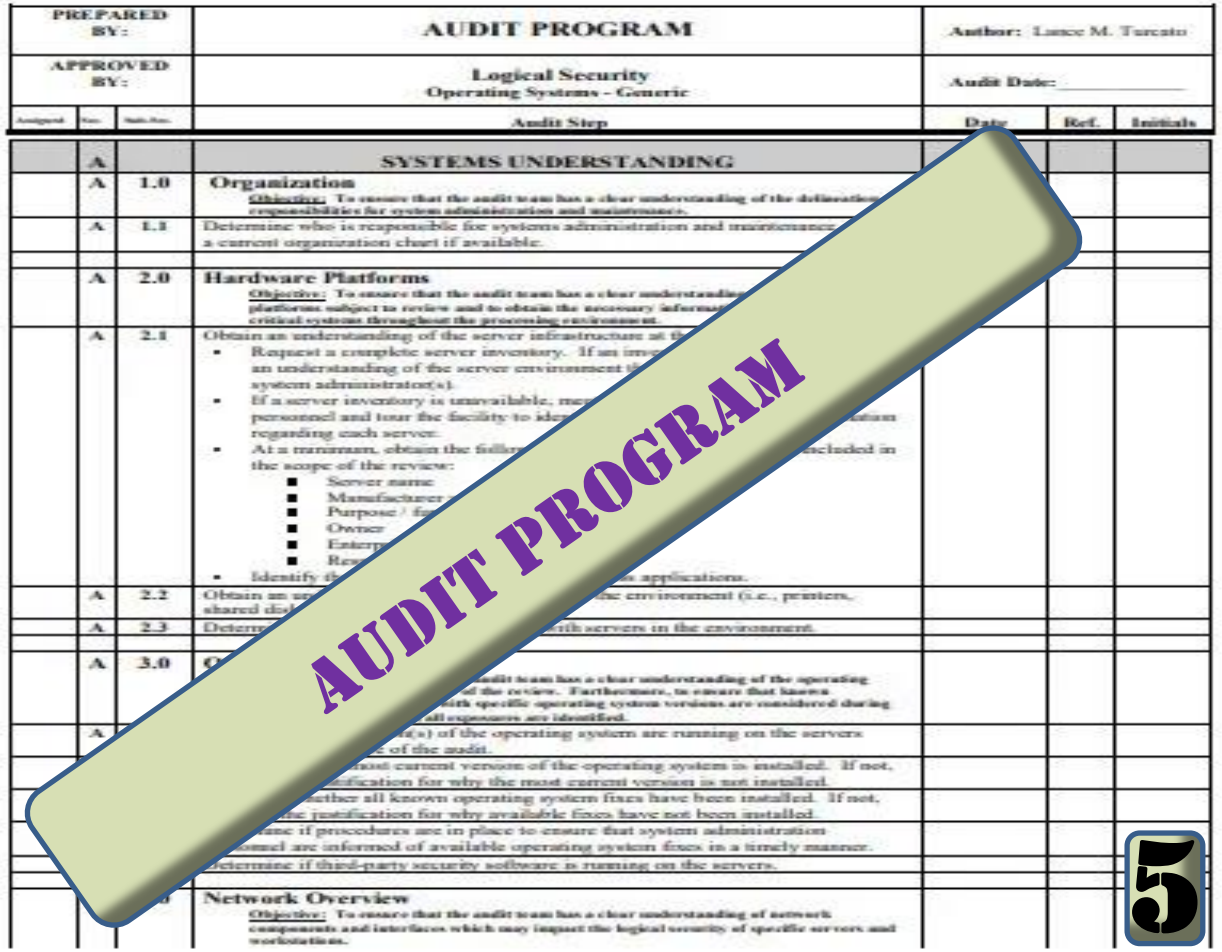
1. Internal Audit Governance Documents –AAWP

IPPF Standard 2010: Planning

The CAE **must** establish a **risk-based plan** to determine the priorities of the internal audit activity, consistent with the organizations goals.

Additional elements of Annual work plan preparations are captured in Section 2 of this presentation

1. Internal Audit Governance Documents –Audit Programs



PREPARED BY:	AUDIT PROGRAM	Author: Lance M. Turcato
APPROVED BY:	Logical Security Operating Systems - Generic	Audit Date: _____

Assigned	Ver.	Walk-Thru	Audit Step	Date	Ref.	Initials
	A		SYSTEMS UNDERSTANDING			
	A	1.0	Organization Objective: To ensure that the audit team has a clear understanding of the delineation responsibilities for system administration and maintenance.			
	A	1.1	Determine who is responsible for systems administration and maintenance a current organization chart if available.			
	A	2.0	Hardware Platforms Objective: To ensure that the audit team has a clear understandi platforms subject to review and to obtain the necessary informa critical systems throughout the processing environment.			
	A	2.1	Obtain an understanding of the server infrastructure at th ▪ Request a complete server inventory. If an inv an understanding of the server environment t system administrator(s). ▪ If a server inventory is unavailable, me personnel and tour the facility to ide regarding each server. ▪ At a minimum, obtain the follo included in the scope of the review: ■ Server name ■ Manufacturer ■ Purpose / fu ■ Owner ■ Enterp ■ Re ▪ Identify th applications.			
	A	2.2	Obtain an u ic environment (i.e., printers, shared dis			
	A	2.3	Determ rk servers in the environment.			
	A	3.0	C udit team has a clear understanding of the operating of the review. Furthermore, to ensure that known with specific operating system versions are considered during all exposures are identified.			
	A		n(s) of the operating system are running on the servers e of the audit.			
	A		most current version of the operating system is installed. If not, tification for why the most current version is not installed.			
	A		whether all known operating system fixes have been installed. If not, the justification for why available fixes have not been installed.			
	A		mine if procedures are in place to ensure that system administration nnel are informed of available operating system fixes in a timely manner.			
	A		Determine if third-party security software is running on the servers.			
	A		Network Overview Objective: To ensure that the audit team has a clear understanding of network components and interfaces which may impact the logical security of specific servers and workstations.			

AUDIT PROGRAM

5

2240 – Engagement Work Program

Internal auditors must **develop** and **document work programs** that achieve the engagement objectives.

Audit programs capture processes in scope, risk, controls [existing & desired] and audit tests

Details to be covered in **Section 2.**

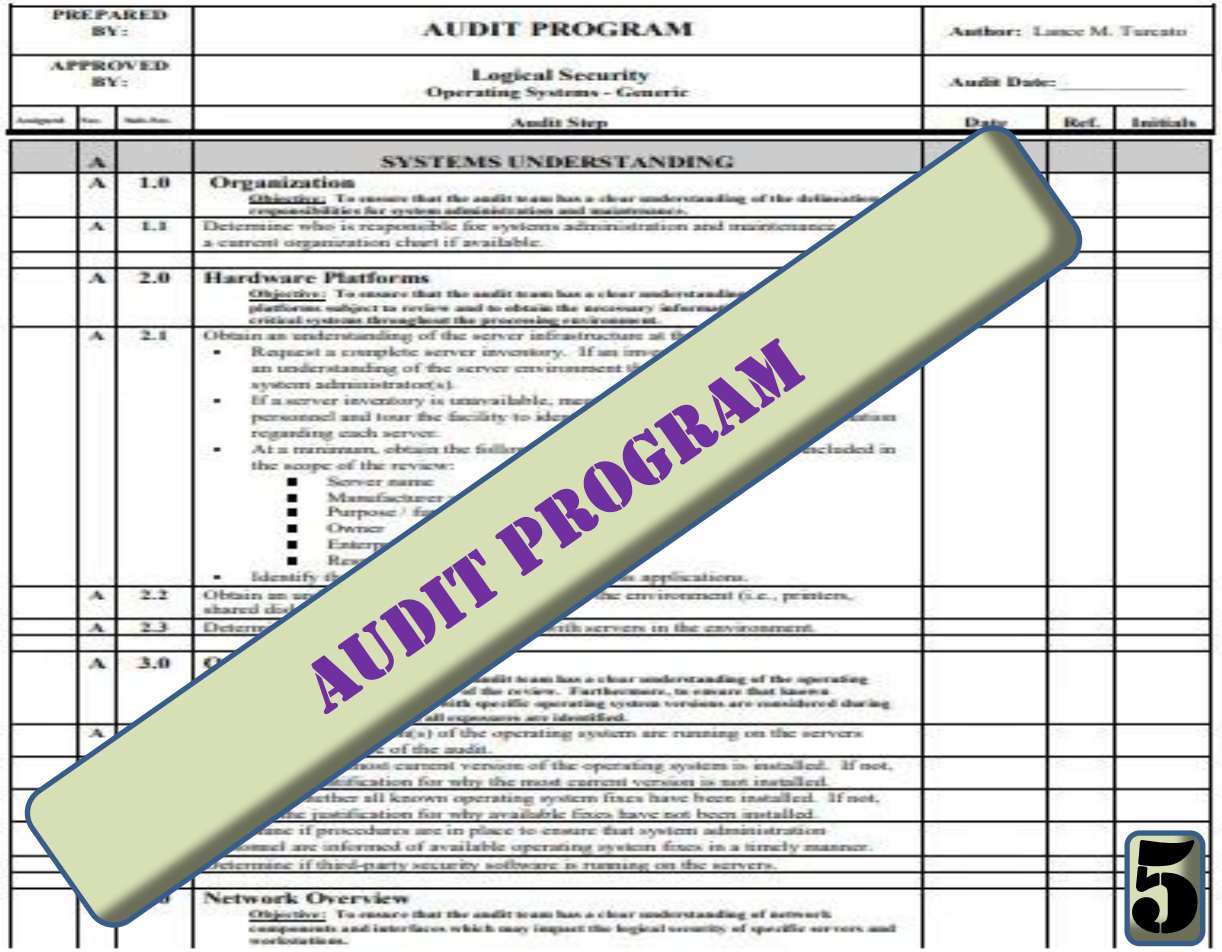
1. Internal Audit Governance Documents –Internal Audit Manual

Standard 2040 – Policies & Procedures

Internal audit policy and procedure documents often are **assembled into an internal audit manual** for the internal audit activity to use. The documents may include methods and tools for training internal auditors.

CAE may require internal auditors to acknowledgement by signature that they have read and understood the manual.

2. Developing audit programs



PREPARED BY:	AUDIT PROGRAM	Author: Lance M. Turcato
APPROVED BY:	Logical Security Operating Systems - Generic	Audit Date: _____

Assigned	Ver.	Walk-Thru	Audit Step	Date	Ref.	Initials
	A		SYSTEMS UNDERSTANDING			
	A	1.0	**Organization** Objective: To ensure that the audit team has a clear understanding of the delineation responsibilities for system administration and maintenance.			
	A	1.1	Determine who is responsible for systems administration and maintenance a current organization chart if available.			
	A	2.0	**Hardware Platforms** Objective: To ensure that the audit team has a clear understandi platforms subject to review and to obtain the necessary informa critical systems throughout the processing environment.			
	A	2.1	Obtain an understanding of the server infrastructure at th ▪ Request a complete server inventory. If an inv an understanding of the server environment t system administrator(s). ▪ If a server inventory is unavailable, me personnel and tour the facility to ide regarding each server. ▪ At a minimum, obtain the follo ▪ Server name ▪ Manufacturer ▪ Purpose / fu ▪ Owner ▪ Enterp ▪ Re ▪ Identify th applications.			
	A	2.2	Obtain an u ic environment (i.e., printers, shared dis			
	A	2.3	Determ h servers in the environment.			
	A	3.0	O udit team has a clear understanding of the operating of the review. Furthermore, to ensure that known with specific operating system versions are considered during all exposures are identified.			
	A		n(s) of the operating system are running on the servers e of the audit.			
			most current version of the operating system is installed. If not, tification for why the most current version is not installed.			
			whether all known operating system fixes have been installed. If not, ific justification for why available fixes have not been installed.			
			ance if procedures are in place to ensure that system administration nnel are informed of available operating system fixes in a timely manner.			
			determine if third-party security software is running on the servers.			
			Network Overview Objective: To ensure that the audit team has a clear understanding of network components and interfaces which may impact the logical security of specific servers and workstations.			

AUDIT PROGRAM

5

"Audit's role in enterprises continues to change in reaction to events, risks, or regulation affecting the company. More time needs to be invested to shift internal audit from reactionary to align with the enterprise's strategic needs."

PwC 2014 State of the Internal Audit Profession Study, March 2014

2. Developing audit programs - Annual planning - AAWP

IPPF Standard 2010: Planning

The CAE **must** establish a **risk-based plan** to determine the priorities of the internal audit activity, consistent with the organizations goals.

The related Practice Advisory 2010-1: Planning

The internal audit activity's plan of engagements **must** be based on a documented on a documented ***risk assessment***, **undertaken at LEAST annually**. The input of senior management and the board must be considered in this process.

Standard 2020: Communication & Approval

CAE **must** communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations.

2. Developing audit programs - Engagement planning

IPPF Standard 2200: Engagement Planning

Internal auditors must develop and document **a plan for each engagement**, including the engagement's objectives, scope, timing, and resource allocations.

Standard 2210: Engagement Objectives

Objectives must be established for each engagement.

2210.A1 – Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

2210.A2 – Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

2210.A3 – Adequate criteria are needed to evaluate governance, risk management, and controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished

2. Developing audit programs - Engagement planning…

In addition to the main planning documents, the following are prepared:

1. Audit notification – before planning
2. Kick off meeting notes/ agenda
3. Tasks Allocation
4. List of requirements

1, 2 and 4 are circulated to auditee early enough as per your service charter

2. Developing audit programs - Audit Programs

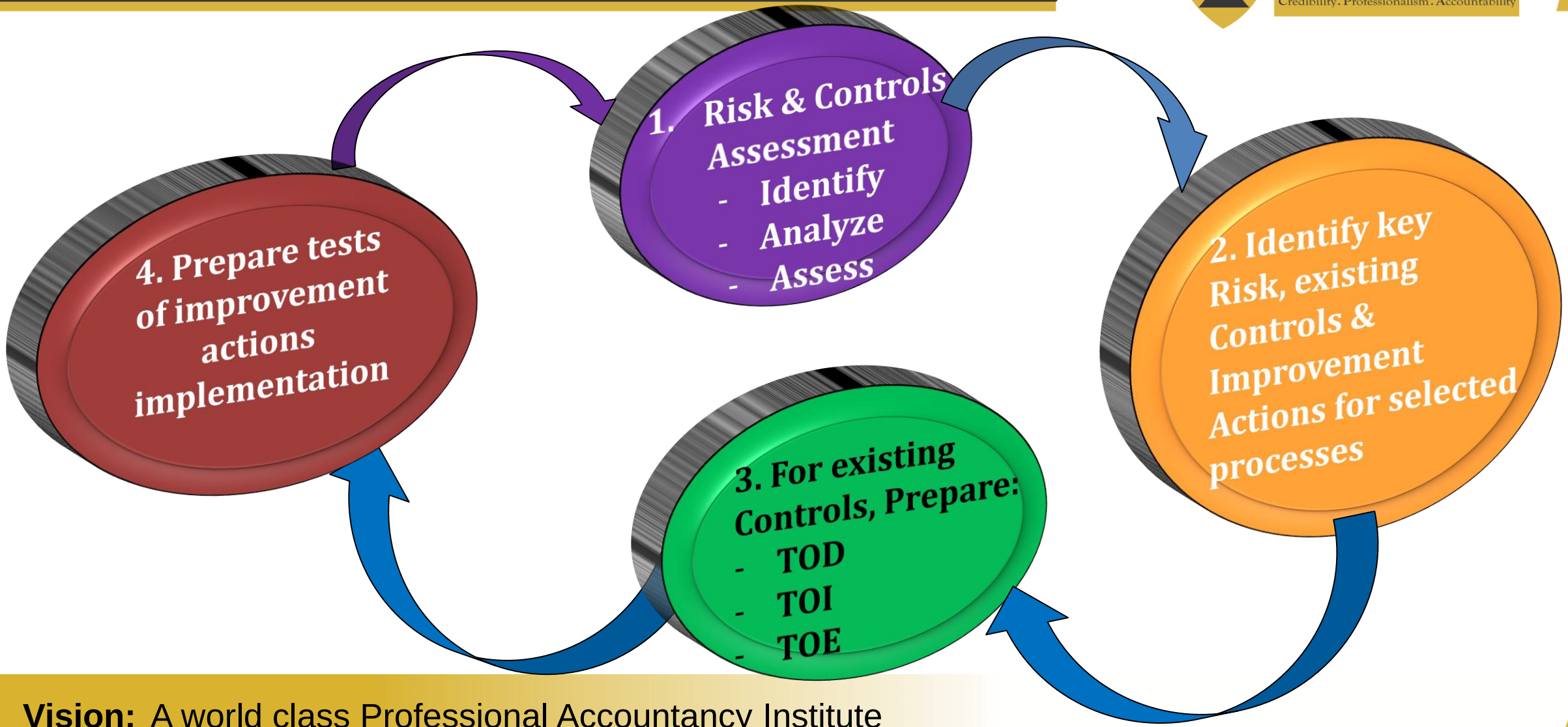
2240 – Engagement Work Program

Internal auditors must **develop** and **document work programs** that achieve the engagement objectives.

2240.A1 – Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement. The work program **must be approved** prior to its implementation, and any adjustments approved promptly.

2240.C1 – Work programs for consulting engagements may vary in form and content depending upon the nature of the engagement.

2. Developing audit programs - Steps



2. Developing audit programs - Audit Programs - RCSA

Process: Procurement

Process objective: To procure goods and services at most cost effective price, required quality and within expected timelines

#	Critical success factors	Cause	Risk event	Effect	Inherent risk rating
1	Procurement system [accurate, available, secure, modern, scalable]	Weak system configurations, overrides	Deleted/ modified LPOs	Suppliers overpayments, lost money	High
2	Goods & services [suitable, quantity, quality, timely delivery]	No specifications, management override	Good procured yet not required	Loss of money	High
3	Procurement staff (adequate, integrity,	Collusion, Weak inspection, low cost objective	Substandard supplies	Unmet objectives, lost money, repeat procurements	High

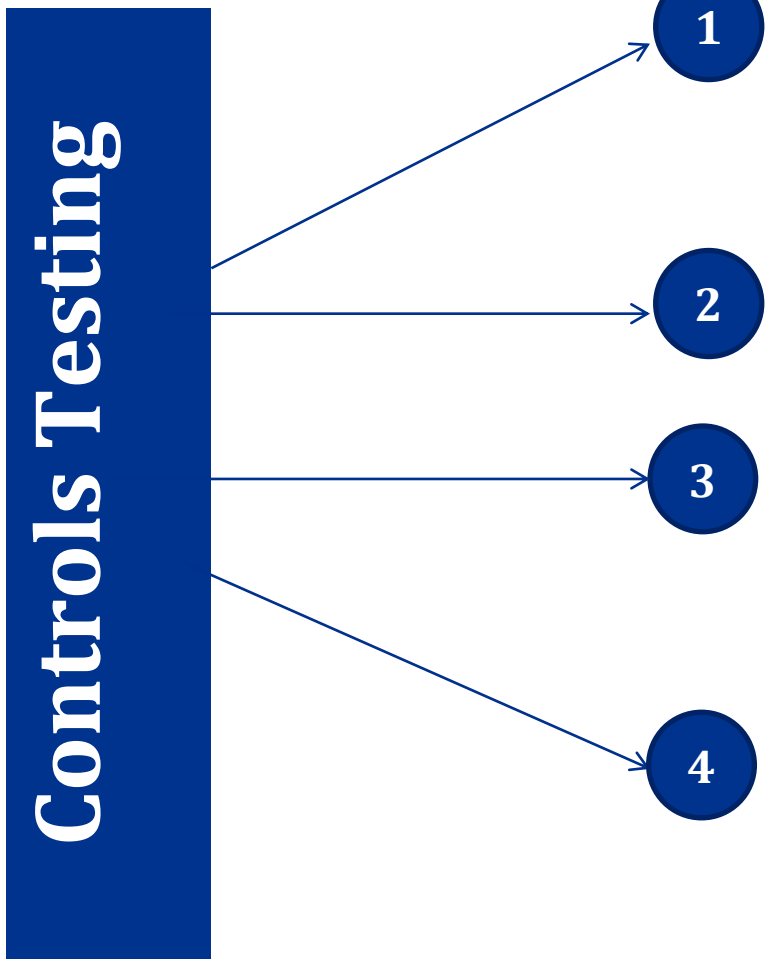
2. Developing audit programs - Audit Programs – RCSA…

#	Cause	Risk event	Effect	IR Rating	Control in place	Residual risk rating
1	Weak system configurations, overrides	Deleted/ modified LPOs	Suppliers overpayments, lost money	High	Maker checker control, sequential numbers generation (Requisitions, LPOs)	Low
2	No specifications, management override	Good procured yet not required	Loss of money	High	Requisition in system, LPOs, Inspection & acceptance,	Medium
3	Collusion, Weak inspection, low cost objective	Substandard supplies	Unmet objectives, lost money, repeat procurements	High	Inspection and acceptance	High

2. Developing audit programs - Audit Programs – RCSA…

#	Risk event	Control in place	RRR	Audit tests/ program
1	Deleted/ modified LPOs	Maker checker control, sequential numbers generation (Requisitions, LPOs)	Low	Will not be tested. Risk within appetite level. To monitor in ERM
2	Good procured yet not required	Requisition in system, LPOs, Inspection & acceptance,	Medium	Will not be tested. Risk within appetite level. To monitor in ERM
3	Substandard supplies	Inspection and acceptance	High	**Test Inspections for each supply** **TOD** – What does Policy or procedure say about this control? **TOI** – Sample 1 transaction and confirm if implemented **TOE** – Analyze data to check consistency or sample and confirm was done in line with procedure.

2. Developing audit programs - Testing approach



Test of Design (TOD)

- Does the control exist in the organization? Is it documented in a policy or procedure?

Test of Implementation (TOI)

- How is it performed and documented?

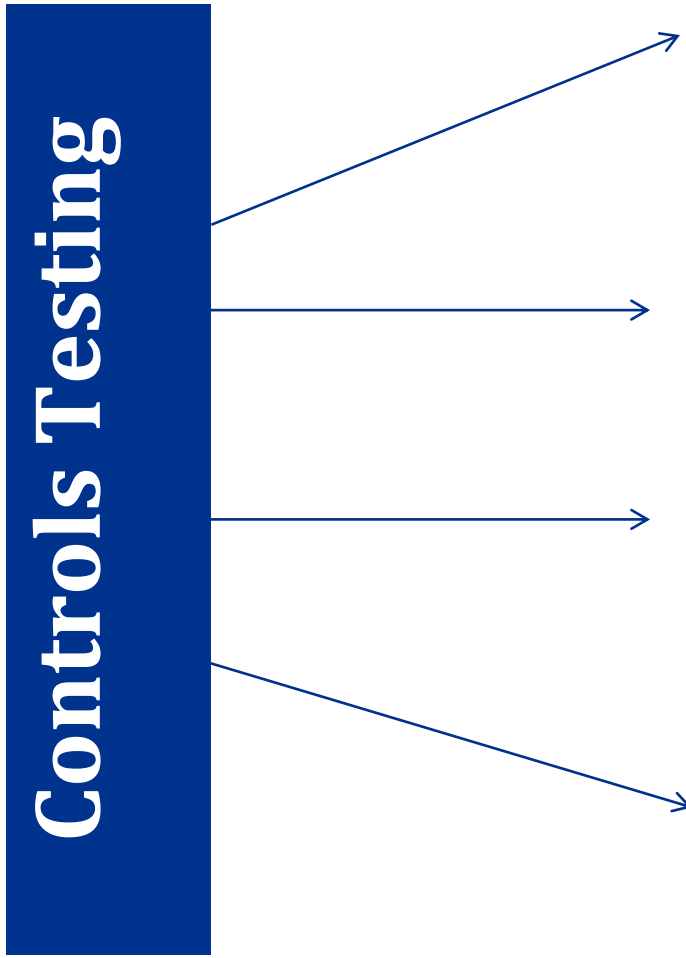
Test of Operating Effectiveness (TOE)

- Has the implemented control/procedure been adequately & consistently applied throughout the period under review?

Improvement Actions

- Have the known improvements actions been implemented on due dates?
- What are the additional improvement actions to mitigate the risk further?

2. Developing audit programs - Testing approach – I&A process



1 - **Test of Design (TOD)**
- Establish if there is a policy or procedure on how procurements inspection and acceptance. If not documented, enquire from process owner

2 - **Test of Implementation (TOI)**
- Select one tender and confirm that the documented procedure was followed

3 - **Test of Operating Effectiveness (TOE)**
- Select a sample of procurements and
- Establish that a committee was established and approved by CEO
- Inspection documented & signed off by all members.

4 - **Improvement Actions**
- Establish if there is rotation of staff who are nominated to perform inspections [no staff does more than 3 inspections in a year].

2. Developing audit programs - Testing approach – I&A process

CAUTION: 

Avoid asking for standard audit programs from your peers **blindly**, instead develop your own risk based assurance programs aligned to your organization enabling legislation, corporate goals, policies and procedures.

Where your organization polices & procedures are deficient/ defective, you can engage management and Board to embrace **leading practices** like ISO Standards, known frameworks e.g. King III, COSO, etc to enhance controls. Once, adopted, these practices need to be included in policies and procedures.


Thank
you

My contacts

Phares Chege

Deputy Commissioner – Internal Audit

Kenya Revenue Authority

Times Tower, 25th Floor

P.O. Box 40160-00100,

Nairobi – Kenya

T: +254 (0)20 281 7055

M: +254 721 411504/ +254 733 411504

Email: phares.chege@kra.go.ke

3. Questions and discussions