Audit Quality Assurance workshop

Risk assessment & Internal controls

by:
CPA Steve Obock
Associate Director- KPMG Kenya
March 2017

Agenda

- Introduction
- Risk Assessment Approaches during Audit
- Internal Control Environment
- Responding to Assessed Risks
- Q&A

Introduction

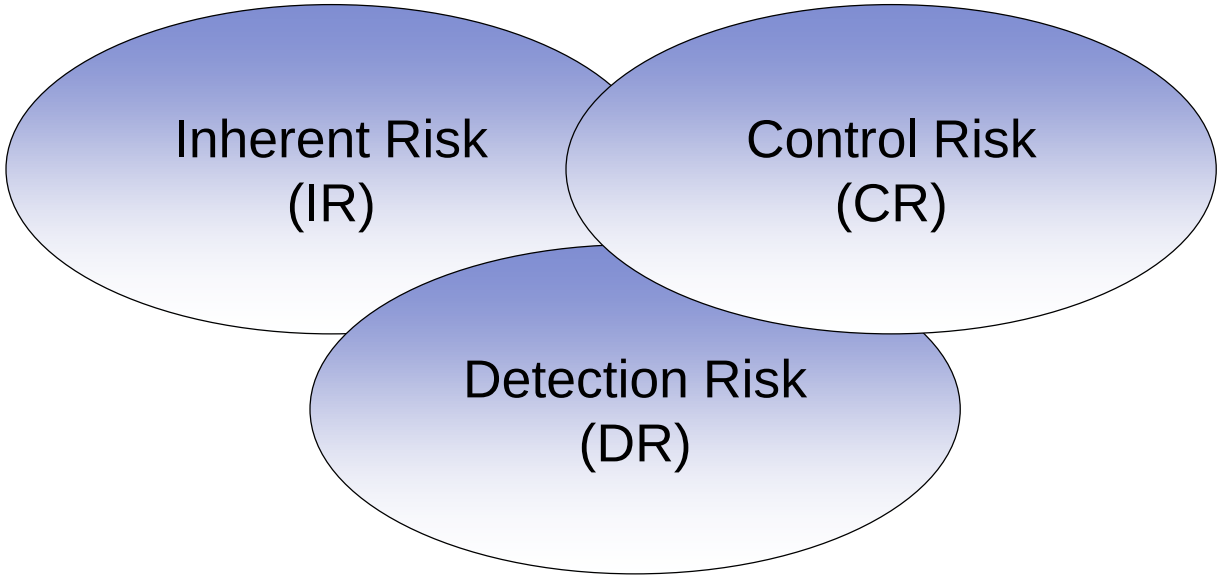
Audit procedures are fundamentally risk based and aimed at reducing the audit risk to acceptable levels.

Audit Risk

	Financial Statements are free of material misstatements	Financial Statements contain material misstatements
Unqualified opinion	✓	*Audit Risk*
Modified opinion	✗	✓

Components of Audit Risk

Audit Risk = Inherent Risk x Control Risk x Detection Risk



Audit Risk = **Risk of Material Misstatement (RoMM) at the assertion level** x Detection Risk

Risk Assessment

What are Risk Assessment procedures?

Audit **procedures** performed to obtain an **understanding of the entity and its environment**, including the entity's internal control, to **identify and assess the risk of material misstatement due to fraud or error**, at the financial statement and assertion levels

Clarified ISA 315.4(d)

Risk Assessment and Planning Discussion

Meeting held with the Engagement Partner and other key members of the engagement team to discuss various Risk Assessment topics.

Professional judgment in deciding:

- ✓ the timing of the discussion ?
- ✓ the agenda for the discussion ?
- ✓ how the discussion is conducted ?
- ✓ communications to team members not participating in the discussion ?
- ✓ the documentation of the discussion ?

Minimum topics in risk assessment

- Understanding the entity
- Emphasis on the risk of fraud
- Identifying and assessing the risk of material misstatements
- Our response to the identified significant risks and other matters
- Other matters to be considered throughout the audit

RoMM = IR + CR

		Control risk	
		Higher	Lower
Inherent Risk	Significant Risk	High	Moderate/Low
	Risk that is not Significant	Moderate/Low	Low

Internal control environment

Internal control:

The process designed, implemented and maintained by those charged with governance & management to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations.

Selection of relevant controls

- **Preventative and detective controls**
- **WCGW**
- **Multiple controls to one WCGW**

Factors to Consider – Identifying relevant controls

We consider:

- WCGW for which the error or fraud could occur
- The nature of the controls implemented by management
- The risk that the control addresses
- The significance of each control in achieving the objectives of the control criteria and whether more than one control achieves a particular objective or whether more than one control is necessary to achieve a particular objective
- The number of different assertions addressed by each control
- The risk that the controls might not be operating effectively

Risk of Failure

For each control selected for testing operating effectiveness, we assess the risk of failure of the controls

Risk of failure is assessed either as higher or lower

In making this assessment, we consider the risk that the control might not be effective and, if not effective, the risk that a material misstatement would result

Factors to consider when assessing the Risk of Failure

- The nature and materiality of the misstatements
- Inherent risk of error, significant account(s) and assertion(s)
- Changes in the volume or nature of transactions
- Competence of the personnel
- Effectiveness of relevant entity level controls and higher level controls

Factors to consider when assessing the Risk of Failure

- Nature and frequency of the control
- Complexity of the control
- History of errors
- Degree of reliance on the effectiveness of other controls
- Manual versus automated control

Procedures for evaluating design and implementation

Evaluating design & implementation ← **the control exists and the entity is using it**

- **Inquiry (alone not sufficient)**
- **Observation**
- **Inspection**
- **Corroborative inquiry**
- **Walkthrough**

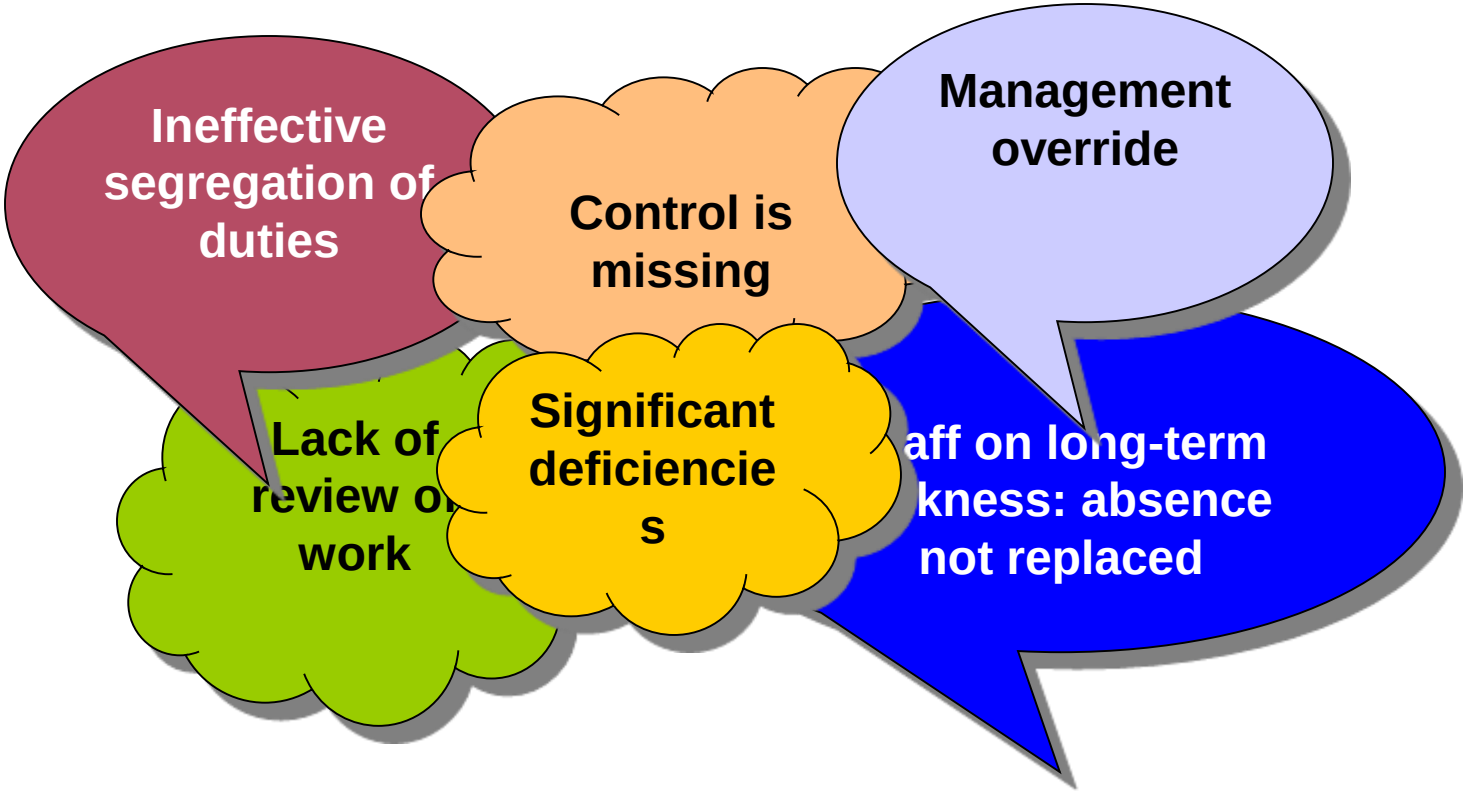
- **Performing walkthroughs is a good way to evaluate the design and implementation of controls.**

What is a Walkthrough?

Effective way to:
Understand the flow of transactions Verify we identified what could go wrong in the process Identify controls management has implemented to address what could go wrong

- **Consists of:**
  - Following a single transaction from origination through the entity's processes
  - Using the same documents and technology as entity personnel
  - A combination of inquiry, observation and inspection

Deficiencies?



Responding to Assessed Risks

- ISA 315 states that ‘’the objective of the auditor is to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels, through understanding the entity and its environment, including the entity’s internal control, thereby providing a basis for designing and implementing responses to the assessed risks of material misstatement’’.

Responding to Assessed Risks

ISA 315.6 provides the following risk assessment procedures:

- Inquiries of management, internal audit function and TCWG.
- Analytical procedures.
- Observation and inspection.

The Entity and Its Environment

The auditor shall obtain an understanding of the following:

- Relevant industry, regulatory, and other external factors including the applicable financial reporting framework.
- The nature of the entity, including:
  - ✓ its operations;
  - ✓ its ownership and governance structures;
  - ✓ the types of investments & strategies
  - ✓ Its structure; and
  - ✓ Financing arrangements

Risk Assessment Approaches:

- Business Risk Model
- Audit Risk Model
- Use of Information Technology

Business Risk Model

Overview:

- Business risk is the risk that a business will not achieve its objectives
- Corporate governance guidelines emphasize the importance of risk management processes within a business
- The business risk model of auditing requires the auditor to consider the entity's process of assessing business risk and the impact this might have in terms of material misstatement

Business Risk

- **Financial Risks** – Risk arising from the company's financial activities or financial consequences of operations. E.g. Going concern, market risks, credit risk, liquidity risks etc.
- **Operating Risks** – Risks arising from the operations of the business. E.g. Loss of orders, loss of key personnel, physical damage to assets, poor brand management, technological change, stock outs, business processes unaligned to objectives.
- **Compliance Risks** – Risks arising from non-compliance with laws, regulations, policies, procedures and contracts.

Audit Risk Model

Overview:

- Audit risk is the risk that the auditors may give an inappropriate opinion when the financial statements are materially misstated
- The risk of material misstatement is made up of inherent risk and control risk
- The audit risk model expresses the relationship between the different components of risk as follows:

Audit Risk = Inherent Risk x Control Risk x Detection Risk

- Business risk forms part of the inherent risk associated with the financial statements
- Information gained in obtaining an understanding of the business is used to assess inherent risk
- Assessment of control risk involves assessing the control environment and control activities

Information Technology and Risk assessment

Overview:

- A huge number of organizations now use computer systems to run their businesses and to process financial information
- The main risks associated with using computerized systems include infection by viruses and access by unauthorized users. Both these risks could potentially have a very damaging effect on the business.
- This means that a number of the controls which the directors are required to put into place to safeguard the assets of the shareholders must be incorporated into the computer systems.
- Auditors have to assess the effectiveness of the controls in place within computer systems and can do this by performing a systems audit as part of their initial assessment of risk during the planning stage of the audit.

Risks associated with the use of computerized systems

The two key business risks of organizations using computerized systems are:

- The system being put at risk by a **virus** or some other fault or breakdown which spreads across the system
- The system being **invaded by an unauthorized user**, who could then:
  - ✓ Affect the smooth operation of the system
  - ✓ Obtain commercially sensitive information

Systems Audit

- As part of any audit, auditors are required to assess the quality and effectiveness of the accounting system. Increasingly, this necessarily includes a consideration of the computer systems in place within the organization.
- The following are the key areas they are likely to concentrate on to establish how reliable the systems are:
  - ✓ Management policy
  - ✓ Segregation of duties
  - ✓ Access rights
  - ✓ Security
  - ✓ Data storage and recovery plans

Overall responses to risk

The auditor should determine **overall responses** to address the risks of material misstatement at the financial statement level.

This may include:

- ✓ Emphasizing to the audit team the need to maintain **professional skepticism** in gathering and evaluating audit evidence.
- ✓ Assigning more **experienced staff**, those with **special skills** or using **experts**
- ✓ Providing **more supervision**
- ✓ Incorporating **additional elements of unpredictability** in the selection of further audit procedures

Interactive Session

Conclusion

Risk assessment is key, and at the Centre of assurance services. It is RISKY when risk assessment is not given due care and attention.

Contacts

Thank you

Stephen Obock
Associate Director
KPMG Kenya

C: 0709 576 129 / 0712 601 624
E: sobock@kpmg.co.ke