Conducting Risk Assessment and Audit of the Internal Control System

(An ICPAK Audit Staff Training Workshop 2016)

Uphold . Public . Interest

Conducting Risk Assessment & Audit of the Internal Control System

About the Presenter: Jona Owitti, CISA

Specialisation / Interest: Information Systems (IS) Auditing; Information Security; Risk and IT Governance

Presenter at: National (e.g., ISACA, ICPAK, IIA) and International (MIS Training, iCPAR)

Now: (a) Chief Trainer – ISACA Kenya Chapter
(b) Founder and Past President – ISACA Kenya Chapter

Past: Chevron Corporation (Caltex) – Regional IS Audit Manager for Africa, Middle East and Pakistan Region

Certification: Certified Information Systems Auditor (CISA)

Education: M.Sc. (Computer Science) (Dundee - UK); B.Ed. (Science) Hons. (Nairobi)

Experience: 30 years of experience in IS Auditing, Risk and Governance across the Globe (Africa, The Americas, Asia, Australia/Oceania, and Europe)

E-mail: jona.owitti@yahoo.com (Personal); jona.owitti@isaca.or.ke (ISACA Kenya Chapter)

Jona Owitti, CISA

Conducting Risk Assessment & Auditing the IC System

Agenda

- Overview / Definitions
- Risk Assessment Process
- Internal Control Environment
- Auditing the Internal Control System; including Implications of IT Environment
- Open Discussion / Conclusion

Conducting Risk Assessment & Auditing the IC System

Overview / Definition

Discussion Notes

Conducting Risk Assessment & Auditing the IC System Risk Management Process

(Source: *Risk Management Standard (AS/NZS 4360: 2004)*)

- **Establish the Context**: for strategic, organisational and risk management and the criteria against which business risks will be evaluated.
- **Identify Risk**: that could 'prevent, degrade, delay or enhance' the achievement of an organisation's business and strategic objectives.
- **Analyse Risk**: consider the range of potential consequences and the likelihood that those consequences could occur.
- **Evaluate Risks**: compare risks against the firm's pre-established criteria and consider the balance between potential benefits and adverse outcomes.
- **Treat Risks**: develop and implement plans for increasing potential benefits and reducing potential costs of those risks identified as requiring to be 'treated'.
- **Monitor and Review**: the performance and cost effectiveness of the entire risk management system and the progress of risk treatment plans with a view to continuous improvement through learning from performance failures and deficiencies.
- **Communicate and Consult**: with internal and external 'stakeholders' at each stage of the risk management process.

Note that: Identify, Analyse and Evaluate Risks are collectively grouped as 'Risk Assessment'.

5

Conducting Risk Assessment & Auditing the IC System (Definition/s)

- Procedures to conduct risk assessment (using RCM):
  - Inquiries with management and others within an organization,
  - Observation and inspection;
  - Review of previous years' audit report; management letters and board minutes; and
  - Business process mapping and identification.

Discussion Notes

6

Conducting Risk Assessment & Auditing the IC System (Definition/s)

- **Internal Control:**
  - The process designed, implemented and maintained by those charged with governance, management and other personnel 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.
  - The term "controls" refers to any aspects of one or more of the components of internal control.

*(**Ref**: International Standard on Auditing (ISA)*

Conducting Risk Assessment & Auditing the IC System

Conducting Risk Assessment

(COSO Perspective)

(Audit Perspective)

Risk Assessment Process (COSO ERM Framework)

- **Risk Assessment Process:**
  - Risk Assessment Process follows **event (risk) identification** and precedes **risk response**.
  - **Purpose:** To assess how big the risks are in order to focus management's attention

(***Ref:*** *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*

Discussion Notes 9

Risk Assessment Process (COSO Perspective)

- **Risk Assessment Process:**
  - Risk Assessment Process **follows** *event identification* and **precedes** *risk response*.
  - Purpose: To assess how big the risks are in order to focus management's attention

(**Risk Assessment** ➔ Develop Assessment Criteria; Assess Risks; Assess Risk Interactions; and Prioritize Risks)

Discussion Notes 10

Risk Assessment Process (COSO Perspective)

- **Identify risks (or events):**
  - A comprehensive list of risks (and opportunities)
  - Organized by risk category (financial, operational, strategic, compliance); and sub-category (market, credit, liquidity, etc.)
  - A universe of risks making up the organization's risk profile
  - Then list undergoes prioritization for senior management and board to focus on key risks (i.e., by performing risk assessment)

Risk Assessment Process (COSO Perspective)

- **Develop assessment criteria:**
  - First activity within the risk assessment process
  - Risks and opportunities are assessed in terms of impact (consequence) **and** likelihood (probability)
  - Additionally, may also evaluate risk along other dimensions such as vulnerability and speed of onset
- **Assess risks:**
  - Assign values to each risk and opportunity using the defined procedure
  - May be accomplished in two stages: qualitative techniques, followed by quantitative analysis of the key risks

Risk Assessment Process (COSO Perspective)

- **Assess risk interactions:**
  - Risks do not exist in isolation
  - A seemingly insignificant risk has the potential, when it interacts with other events and conditions, to cause great damage or create significant opportunity
  - So, organizations are increasingly considering integrated or holistic view of risks e.g., risk interaction matrices
- **Prioritize risks:**
  - Determine risk management priorities
  - Risk is viewed in terms of financial impact and probability
  - ALSO, use subjective criteria such as health and safety impact, reputational impact, and vulnerability

Risk Assessment Process (COSO Perspective)

- **Respond to risks:**
  - Result of risk assessment process is the primary input to a risk response
  - Response options are examined (accept, reduce, share, or avoid)
  - Cost-benefit analysis is performed
  - A response strategy is formulated
  - Risk response plans are developed

Risk Assessment Process
(Risk Interaction Matrix)

	Risk 1	Risk 2	Risk 3	Risk 4 ..	Risk n
Likelihood (1 ... 5)	5	4	3	3	1
Consequence (1 ... 5)	4	4	4	2	1
Risk 1		5	5	0	0
Risk 2	5		3	0	0
Risk 3	5	4		2	0
Risk 4 ..	3	0	0		0
Risk n	0	2	4	0	
Risk Interaction Score	13	11	12	2	0
Risk Interaction Weighted Score	52	44	48	4	0

Discussion Notes 15

Conducting Risk Assessment & Auditing the IC System

Conducting Risk Assessment

(COSO Perspective)

(Audit Perspective)

Discussion Notes 16

Risk Assessment Process
(Discuss – from Audit Perspective)

- **Risk Assessment (Audit Units):**
  - Audit Risk Universe
  - Annual Audit Plan
  - Unit Audit Plan (may use audit tools – e.g., ACL / IDEA

(Discuss Audit Plan with stakeholders)

- Note:
  - Two elements of risk: Impact / Consequence vs Likelihood / Probability)

Conducting Risk Assessment & Auditing the IC System
(Audit Process: Especially for Internal Audit Function)

Plan
- Obtain the background information
- **Perform a risk assessment ('Annual' & 'Individual')**
- Plan the audit schedule
- Select the audit team
- Meet with the clients
- Develop (Update) the audit program

Conduct Audit
- Conduct kick-off meeting to discuss scope, schedule & reporting; and introduce audit team
- Start fieldwork

Reporting
- Formally document findings in the report (may arrange findings by high, medium & low risks)
- Report to include: Background, scope, and objectives
- Report to include: Findings, risk, policy/standard, recommendation, management response (Agree / Action-by, target action date)

Follow-up
- A critical step. Usually starts after six (6) months or a year
- May include a level of fieldwork
- A follow-up memo needed to describe status of findings

Conducting Risk Assessment & Auditing the IC System

Auditing Internal Control System
(Overview)

Auditing of Internal Control System

- **Internal Control Risk Assessment:** Per COSO ERM framework, internal control consists of five (5) integrated components:
  - Control environment
  - Risk assessment
  - Control activities
  - Information and Communication
  - Monitoring Activities

Auditing of Internal Control System

- Risks faced by business, include:
  - Industry risk
  - Strategic risk
  - Operation risk
  - Compliance risk
  - Financial risk
- Significant risks may lead to loss of profits or bankruptcy, e.g.,
  - An example of industry risk: The film giant Kodak filed for bankruptcy after consumers embraced the newer technology of digital cameras and the film era ended.

Auditing of Internal Control System

- Internal Control Risks:
  - Risks that affect the effectiveness and efficiency of internal controls
  - Affect the achievement of objectives
  - They are a part of operation risk and compliance risk.
- Common internal control risks in business include:
  - lack of sound internal control environment,
  - poorly designed business processes,
  - IT security risk,
  - integrity and ethic risk,
  - human errors and fraud risk, etc.

Conducting Risk Assessment & Auditing the IC System

Auditing Internal Control System
(Auditing)

Auditing of Internal Control System

- Internal Controls:
  - are normally composed of **policies**, **procedures**, **practices** and **organizational structures** that are implemented to reduce risk to the organization.
- Internal controls address:
  - What should be achieved?
  - What should be avoided?

*(**Discuss:** Auditing of Internal Controls to ensure risk is reduced)*

Auditing of Internal Control System
(Control Classifications)

Control Classifications: Preventive, Detective, and Corrective

- Preventive Controls:
  - Detect problems before they arise;
  - Monitor both operation and inputs;
  - Attempt to predict potential problems before they occur and make adjustments;
  - Prevent an error, omission or malicious act from occurring;
  - Segregate duties (deterrent factor);
  - Control access to physical facilities; and
  - Use well-designed documents (prevent errors).

Auditing of Internal Control System
(Control Classifications)

Control Classifications: Preventive, Detective, and Corrective

- Detective Controls:
  - Use controls that detect and report the occurrence of an error, omission or malicious act.
- Corrective Controls:
  - Minimize the impact of a threat;
  - Remedy problems discovered by detective controls;
  - Identify the cause of a problem;
  - Correct errors arising from a problem; and
  - Modify the processing system(s) to minimize future occurrences of the problem.

(Audit work should verify that the business objectives will be achieved and undesired events will be prevented, detected or corrected.)

Conducting Risk Assessment & Auditing the IC System

Auditing Internal Control System

(The IT Environment)

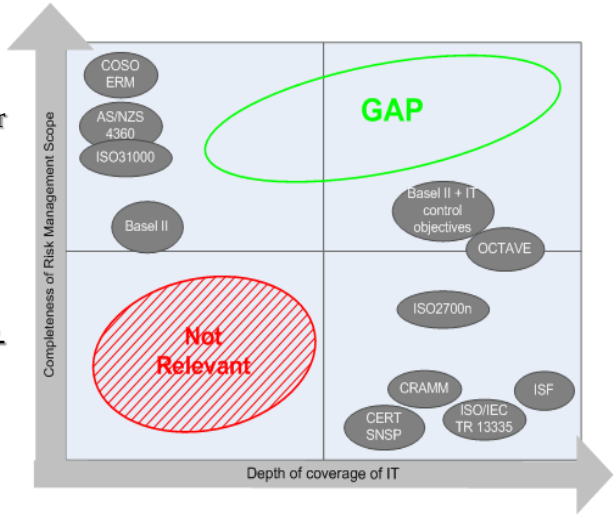
Conducting Risk Assessment & Auditing the IC System

(Technology has complicated the ERM Environment)

Until Recently:
Standards and frameworks are available, but are either too:

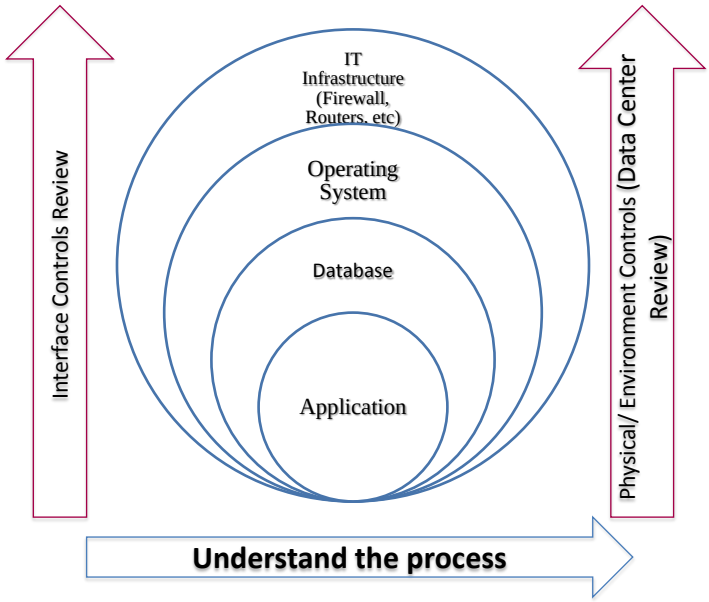
- Generic enterprise risk management-oriented
- IT security-oriented

No comprehensive IT-related risk framework available – until now (e.g., ISACA's Risk IT Framework).



***Source**: ISACA*

Conducting Risk Assessment & Auditing the IC System
(Internal Control System – An IT Environment)



Conducting Risk Assessment and Auditing the Internal Control System

CPAK
Uphold Public Interest

Open Discussion / Conclusion

Thank You

Jona Owitti, CISA
Chief Trainer, ISACA Kenya Chapter
(Cellphone: +254-722-742525)

E-mail address: jona.owitti@yahoo.com (Personal); jona.owitti@isaca.or.ke (Official)

Jona Owitti, CISA