Corporate Governance & Risk Management
Role of Management and the Board

Presentation Made
at the
2nd ICPAK Corporate Governance Conference
Wednesday, 10th April 2013
Leisure Lodge, Mombasa – Kenya

Jona Owitti, CISA (*jona.owitti@yahoo.com*)
Membership Director – ISACA Kenya Chapter ***(Website:*** *www.isaca.or.ke* ***)***
and
Director, Security Risk Solutions Limited *(www.securityrisk-solutions.com)*

1

Corporate Governance and Risk Management

About the Presenter: Jona Owitti, CISA

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

Presenter at: National (e.g., ICPAK, IIA) and International (e.g., MISTI)

Now: Security Risk Solutions Ltd – Director, Government & Public Sector
ISACA Kenya Chapter – Membership Director

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); B.Ed (Science) (Nairobi)

Experience: 27 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@securityrisksolutions.net (Office)

2

Agenda / Coverage

Corporate Governance and Risk Management

Session (1.5 Hours)

- Overview of Corporate Governance & Risk Management
- Role of the Board and other Stakeholders in RM
- Conclusion / Q&A

3

Corporate Governance & Risk Management

Introduction to Corporate Governance

Overview / Definitions

4

Corporate Governance and Risk Management

Corporate Governance: Sample Definitions

- "The system by which companies are directed and controlled" – *Adrian Cadbury, 1992*
- "The structures, processes, cultures and systems that engender the successful operation of the organisation" – *K Keasey and M Wright, 1993*
- "The process of supervision and control intended to ensure that the company's management acts in accordance with the interests of Shareholders" – *J Parkinson, 1994*

5

Corporate Governance and Risk Management

Components of Corporate Governance

- Ethics
- Integrity
- Good management practices
- Accountability (e.g., financial)
- Information
- Responsibility
- Investment protection
- Shareholder action
- Transparency
- Internal control systems
- Laws

6

Corporate Governance and Risk Management

Corporate Governance – Separation of Duties (SoD):

- Chief Executive Officer (CEO) – responsible for managing the enterprise
- Chairman – responsible for managing the board
- Generally, it is prudent not to appoint the CEO as Chairman without a reasonable period outside the organisation.

7

Corporate Governance and Risk Management

Why is Corporate Governance vital?:

- Even best-run organisations can make mistakes or poor decisions on e.g., investment, recruitment, etc.
- While risk is an important and unavoidable component of modern management, it should not imply that governance of enterprises is overlooked.
- A good decision that leads to e.g., a successful investment can be based on poor assessment of risk. Also, good governance practice can lead to poor decision making. Hence, there must be a balance.
- Investors and other stakeholders need assurance that senior management are acting in the best interests of the enterprise.

8

So, it is about effective leadership *(see next slide)*

Corporate Governance & Risk Management
Leadership Beyond Governance

Leadership: Definition

- Northouse (2007) defines Leadership as:
  - "a process whereby an individual influences a group of individuals to achieve a common goal."

Governance: Definition

- The IIA standards define governance as:
  - "the combination of processes and structures implemented by the board to inform, direct, manage and monitor the activities of the organization towards the achievement of its objectives."

9

Corporate Governance & Risk Management
Leadership Beyond Governance

Concept of Leadership:

- Eight (8) qualities of a good leader:
  - Unwavering courage
  - Exercises self-control
  - A keen sense of justice
  - Definite vision and plan (plans his/her work and works his/her plan)
  - The habit of doing more than paid for
  - Mastery of details
  - A pleasant personality
  - Cooperation

10

Corporate Governance and Risk Management

Introduction to Risk Management

Overview / Definitions / Principles

11

Risk Management (Overview / Definitions)

- **Risk**
  - defined in ISO 31000 as *the effect of uncertainty on objectives* (whether positive or negative)
  - ISO 27005 states: “risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation”.
  - NIST SP 800-30 states: “risk is a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability and the resulting impact of that adverse event on the organisation”.

12

Risk Management (Overview / Definitions)

Essential Components of Risk Management (RM)

- **Risk Capacity** - the maximum amount of risk that can be supported by a company, expressed as a sum of money. Determined by available capital, earnings strength/stability
- **Risk Appetite** - Amount of risk that management are willing to take, given risk capacity, strategic business objectives and culture. Risk Appetite serves as an overall guide to resource and capital allocation.
- **Risk Limits** - Allocation of Appetite (in metrics relevant to a specific risk) to business units and functions. Reflect expected returns and risks.

13

Enterprise Risk Management
Risk Appetite and Risk Tolerance

Risk Appetite (Definition):

- The amount of risk that an organisation is willing to seek or accept in the pursuit of its long term objectives.

- In contrast to Risk Tolerance (see below), Risk Appetite is about what the organisation does want to do and how it goes about it. So, it is the board's responsibility to define risk appetite.

14

Enterprise Risk Management
Risk Appetite and Risk Tolerance

Risk Tolerance (Definition):

- The boundaries of risk taking outside of which the organisation is not prepared to venture in the pursuit of its long term objectives.

- Risk tolerance can be expressed in terms of absolutes, e.g., "we cannot expose more than x% of our capital to losses in a certain line of business" or "we will not deal with certain types of customers"

15

Enterprise Risk Management
Risk Appetite and Risk Tolerance

Risk Appetite vs Risk Tolerance:

- **Risk Appetite** is about the pursuit of risk

  while

- **Risk Tolerance** is about what you can allow the organisation to deal with.

- Generally, risk appetite (RA) will be smaller than risk tolerance (RT). In turn, risk tolerance will be smaller than risk universe (RU).

  Thus, RA is a subset of RT and RT is a subset of RU

16

Risk Management (Overview / Definitions)

- **Risk Management**
  - identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.
- **Enterprise Risk Management (ERM)**
  - "… a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Source: COSO Enterprise Risk Management – Integrated Framework. 2004. COSO.

17

Risk Management (Overview / Definitions)

- **Strategic Risk Management**
  - a process designed to keep both the risks associated with doing business and the costs to a minimum
  - could be an indication to insurance underwriters that an organisation has performed a thoughtful analysis of the risks involved in doing business – hence, may maximize the chances of obtaining affordable insurance.

18

Risk Management (Overview / Definitions)

- **Operational Risk Management (ORM)**
  - The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events." – Basel Committee
  - Benefits of ORM
    - Reduction of operational loss.
    - Lower compliance/auditing costs.
    - Early detection of unlawful activities.
    - Reduced exposure to future risks.

19

Risk Management (Why is RM Important? – Principles)

- **Principles of Risk Management**
  - ISO 31000* states that risk management should:
    - create value
    - be an integral part of organizational processes.
    - be part of decision making.
    - explicitly address uncertainty.
    - be systematic and structured.
    - be based on the best available information.
    - be tailored.
    - take into account human factors.
    - be transparent and inclusive.
    - be dynamic, iterative and responsive to change.
    - be capable of continual improvement and enhancement.

* - An international standard for Risk Management (published on 13Nov09)
Also, ISO 31010 on Risk Management Techniques (pub. 01Dec09)

20

Risk Management
(How do we find risk?)

- There are two elements of a risk
  - The Consequence (also called **impact**) when a risk occurs.
  - The Likelihood (also called **probability**) of the risk occurring

21

Enterprise Risk Management

PAUSE

– ERM Highlights / Overview –

(COSO ERM Cube)

22

Enterprise Risk Management
Types of Risk Businesses Face

Main categories of risk:

- Strategic
  - e.g., a new competitor into the market
- Compliance
  - e.g., introduction of a new legislation
- Financial
  - e.g., increased interest charges on a business loan or non-payment by a customer
- Operational
  - e.g., loss / theft of key equipment

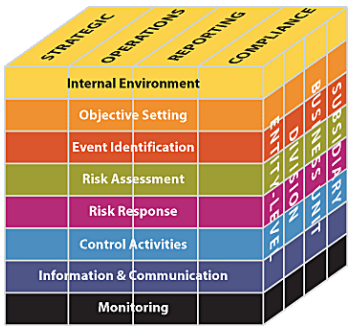
(See ERM Cube below for COSO depiction)

23

Enterprise Risk Management
Categories of Risk as depicted by COSO

ERM is a process to help achieve objectives across the enterprise – i.e.:

- Strategic
- Operations
- Reporting
- Compliance



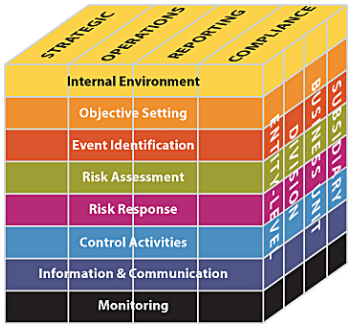
(Source: COSO)

24

Enterprise Risk Management
Why implement risk management?
(Link Between Risk and Org Objectives)

ERM is applied at all levels of the organisation – i.e.:

- Enterprise-level
- Division
- Business Unit
- Subsidiary



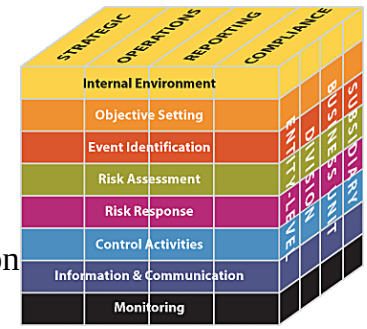
(Source: COSO)

25

Enterprise Risk Management
Categories of Risk as depicted by COSO

Eight (8) interrelated components are identified – i.e.:

- Internal environment
- Objective setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information & Communication
- Monitoring



(Source: COSO)

26

Enterprise Risk Management
Internal Environment

- Establishes a philosophy regarding risk management. Recognises that unexpected as well as expected events may occur
- Establishes the entity's risk culture
- Considers all other aspects of how the organisation's actions may affect its risk culture

27

Enterprise Risk Management
Objective Setting

- Is applied when management considers risks strategy in the setting of objectives
- Forms the risk appetite of the entity — a high-level view of how much risk management and the board are willing to accept
- Risk tolerance, the acceptable level of variation around objectives, is aligned with risk appetite

28

Enterprise Risk Management
Event Identification

- Differentiates risks and opportunities
- Events that may have a negative impact represent risks
- Events that may have a positive impact represent natural offsets (opportunities), which management channels back to strategy setting

29

Enterprise Risk Management
Event Identification *(cont'd)*

- Involves identifying those incidents, occurring internally or externally, that could affect strategy and achievement of objectives
- Addresses how internal and external factors combine and interact to influence the risk profile

30

Enterprise Risk Management
Risk Assessment

- Allows an entity to understand the extent to which potential events might impact objectives
- Assesses risks from two perspectives:
  - Likelihood
  - Impact
- Is used to assess risks and is normally also used to measure the related objectives

31

Enterprise Risk Management
Risk Assessment *(cont'd)*

- Employs a combination of both qualitative and quantitative risk assessment methodologies
- Relates time horizons to objective horizons
- Assesses risk on both an inherent and a residual basis

32

Enterprise Risk Management
Risk Response

- Identifies and evaluates possible responses to risk
- Evaluates options in relation to entity's risk appetite, cost vs. benefit of potential risk responses, and degree to which a response will reduce impact and/or likelihood
- Selects and executes response based on evaluation of the portfolio of risks and responses

33

Enterprise Risk Management
Control Activities

- Policies and procedures that help ensure that the risk responses, as well as other entity directives, are carried out
- Occur throughout the organization, at all levels and in all functions
- Include application and general information technology controls

34

Enterprise Risk Management
Information and Communication

- Management identifies, captures, and communicates pertinent information in a form and timeframe that enables people to carry out their responsibilities
- Communication occurs in a broader sense, flowing down, across, and up the organization

35

Enterprise Risk Management
Monitoring

- Effectiveness of the other ERM components is monitored through:
  - Ongoing monitoring activities
  - Separate evaluations
  - A combination of the two

36

Enterprise Risk Management

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'.

37

Enterprise Risk Management

PAUSE

– Next Slides –

Sources of Risk

38

Enterprise Risk Management
Sources of Risk (defined)

- *Sources of risk* are defined by the ISO as elements which alone or in combination have "the intrinsic potential to give rise to risk" [ISO, 2009]

39

Enterprise Risk Management
Sources of Risk

Sources of Risk:

- External Risks
- Internal Risks

40

Enterprise Risk Management
Sources of Risk

Sources of Risk:

- External Risks – arising from e.g.,:
  - Climate change
  - Customer needs / wants
  - Economy
  - Financial markets
  - Competitor
  - Natural hazard / catastrophe
  - Public relations
  - Regulatory / Legal
  - Shareholder expectations
  - Technological innovation

41

Enterprise Risk Management
Sources of Risk

Sources of Risk:

- Internal Risks – arising from e.g.,:
  - **Strategic**: e.g., Acquisitions, Governance Structure, Reputation, Trademark / Brand Erosion
  - **Operational**: e.g., Management Information (e.g., completeness & accuracy), Human Capital (e.g., skills), Integrity (e.g., conflict of interest), and Technology (e.g., CIA)
  - **Financial** (e.g., misstatement)

42

Enterprise Risk Management
Sources of Risk

Sources of risk (in a financial operation):

- Market prices – exposure to changes in e.g., interest rates, exchange rates, and commodity prices.
- Actions of, and transactions with, other organisations – e.g., vendors, customers, and counterparties in derivatives transactions.
- Internal actions or failures of the organisation – e.g., people, processes, and systems.

43

Enterprise Risk Management
Sources of Risk

Sources of risk (in an agricultural operation):

- Production Risk – yield / quality variability
- Marketing Risk – changes in price / external conditions
- Financial Risk – variability in debt / equity capital and ability to meet cash demands
- Legal Risk – responsibility for contracts, statutory compliance, and business structure
- Human Resource Risk – managing people

Note: Strategic planning is critical for the overall success of any operation

44

Corporate Governance & Risk Management
Role of Board and Other Stakeholders in RM

PAUSE

– Next Slides –

Role of the Board and Other Stakeholders in RM

45

Role of Board/Other Stakeholders
Who manages risks?

Board of Directors	**Provides oversight** (details provided in slides below)
Board Risk Management Committee	Approves risk management policies Evaluate management of risks "Big Picture" analysis of risk trends
Senior Management	**Manages and monitors risk**
Executive Committees	Assists Senior Management monitor risk
Audit and Compliance	**Audit – Provides independent assurance** **Compliance – Provides independent review**
Risk Management	Assists in setting policies and standards that reflect the risk appetite of the organisation
Business Units	Responsible for owning and managing risk Set and implement policy consistent with enterprise-level policy

46

Risk Management
Role of the Board (BAC may have a role here)

Board Oversight (Four Areas):

- Understand the entity's risk philosophy and concur with the entity's risk appetite
- Know the extent to which management has established effective enterprise risk management of the organisation
- Review the entity's portfolio of risk and consider it against the entity's risk appetite
- Be apprised of the most significant risks and whether management is responding appropriately

(Source: COSO's *Enterprise Risk Management – Integrated Framework*)

47

Risk Management
Role of the Board

Direction from the Top (An Internal Audit example)
– First question to consider:

- What are internal auditors being asked to do?
- Thus, it is vital to understand the direction being provided by the Board of Directors – typically through:
  - the **audit committee** (to whom most internal audit activities report functionally), and
  - **management** (to whom most internal audit activities report administratively)

48

Risk Management
Role of the Board / BAC

In August 2009, a Global Audit Information Network (GAIN) Flash Survey, with 321 respondents, identified the following when it asked about the direction provided by the audit committee:

Has the audit committee asked internal auditing …	Yes (%)	No (%)
to provide an opinion on any individual programs or areas related to risk management?	41	59
to provide an opinion on the organisation's overall risk management processes?	23	77
to perform specific audits of any components of risk management?	28	72
for recommendations or advice on enhancing the organisation's risk management processes?	45	55

Source: IIA GAIN Flash Survey, *Internal Auditing's Role in Risk Management, Aug 2009.*

49

Risk Management
Role of the Board / BAC

The above survey data indicate that audit committees may not have high expectations as to what role internal auditors should play – viz:

- Less than half look to internal auditing to provide advice on risk management processes, and
- Just more than a quarter have requested internal auditing to perform specific audits of risk management components.
- It is also noted that expectations regarding rendering opinions on the overall risk management process (23 percent) or individual risk management areas (41 percent) are relatively low.

50

Risk Management
Role of the Board / BAC

One reason for the survey figures not being higher could be found in responses to the survey question below:

How much do you agree or disagree that there is an emerging need for the audit committee to have better insight into the organisation's risk management processes?		
Strongly Agree	**37%**	¾ of the respondents believed that there is an emerging need for audit committees to gain more insight into risk management processes.
Agree	38%	
Neutral	5%	
Disagree	1%	
Strongly Disagree	19%	

Source: IIA GAIN Flash Survey, *Internal Auditing's Role in Risk Management, Aug 2009.*

51

Risk Management
Role of the Board / BAC

From the table above, it can be presumed that a lack of general awareness and understanding about risk management:

- results in a lower level of appreciation of how internal audit activities can provide meaningful insights and assurance surrounding risk management activities.

  It is also likely that audit committees do not perceive that internal auditors possess the right skills and experience to assess risk management activities.

52

Risk Management
Role of Management, Internal Audit, and Audit Committee

PAUSE

– Next Slides –

Roles (cont'd)

53

Risk Management
Role of Internal Audit

Core internal audit roles in regard to ERM:

- Giving assurance on the risk management processes
- Giving assurance that the risks are correctly evaluated
- Evaluating risk management processes
- Evaluating the reporting of key risks
- Reviewing the management of key risks

54

Risk Management
Role of Internal Audit

Legitimate internal audit roles with safeguards:

- Maintaining & developing the ERM framework
- Consolidated reporting on risks
- Championing establishment of ERM
- Coordinating ERM activities
- Coaching management in responding to risks
- Developing ERM strategy for board approval
- Facilitating identification & evaluation of risks

55

Risk Management
Role of Internal Audit

Roles internal auditing should not undertake:

- Setting the risk appetite
- Imposing risk management processes
- Management assurance on risks
- Taking decisions on risk responses
- Implementing risk responses on management's behalf
- Accountability for risk management

56

Enterprise Risk Management

PAUSE

– Next Slides –

ERM Techniques in Strategy Setting

57

Enterprise Risk Management
ERM & Strategy

Strategy (Definition):

- A plan of action designed to achieve a long-term or overall aim (*Oxford Dictionary*)
- A plan that is intended to achieve a particular purpose (*Oxford Advanced Learner's Dictionary*)
- A strategy is a general plan or set of plans intended to achieve something, especially over a long period. (*Collins Dictionary*)
- Strategy is a high level plan to achieve one or more goals **under conditions of uncertainty**. (*Wikipedia*)

58

Enterprise Risk Management
ERM & Strategy

Strategy (Definition):

- Business strategy:
  - is a set of guiding principles that, when communicated and adopted in the organization, generates a desired pattern of decision making
- A strategy is about how people throughout the organization should make decisions and allocate resources in order accomplish key objectives

59

Enterprise Risk Management
ERM & Strategy

Strategy (Definition):

- A strategy is **not** a Mission:
  - "Mission" is what leaders of an organisation want strategy to accomplish;
  - Missions get elaborated into specific goals and performance metrics
- A strategy is **not** the value network:
  - "Value Network" – the web of relationships with suppliers, customers, employees, and investors
- A strategy is not a Vision:
  - "Vision" is an inspiring portrait of what it will look and feel like to pursue and achieve the organisation's mission & goals

60

Enterprise Risk Management
ERM & Strategy

In Summary:

- Mission is about **what** will be achieved;
- The value network is about with **whom** value will be created and captured;
- Strategy is about **how** resources should be allocated to accomplish the mission in the context of the value network; and
- Vision (and incentives) is about **why** people in the organisation should feel motivated to perform at a high level.
- Mission + Network + Strategy + Vision: define the **strategic direction** for a business. They provide the **what**, **who**, **how**, and **why** it is necessary to powerfully align action in complex organisations.

HENCE, THE RISKS!!

61

Enterprise Risk Management
ERM & Strategy

Diagrammatic Illustration of Mission, Network, Strategy & Vision

Source: Demystifying Strategy: The What, Who, How, and Why (Michael Watkins)

62

Enterprise Risk Management
ERM & Strategy

Implication of the above definitions / explanation:

- Cannot develop a strategy for a business without first thinking through mission and goals
- Also, cannot develop a coherent strategy in isolation from decisions concerning the network of partners
- By focusing on all four elements (Mission, Network, Strategy and Vision) and sequencing them correctly, the process of crafting strategy can be demystified

63

Enterprise Risk Management
ERM in Strategy-Setting

- Strategic Risk Management: a process designed to keep both the risks associated with doing business and the costs to a minimum *(re-visited; defined earlier)*
- Strategic risks can undermine an organisation's business model and competitive advantage.
- These risks can arise from within an organization, and they can also develop externally in the business environment.
- Strategic risks are difficult to spot and can even be difficult to imagine.

64

Enterprise Risk Management
ERM in Strategy-Setting

Connecting Risk Assessment and Strategy-setting:

- Strategic risks are difficult to handle. Protiviti identifies four (4) reasons for the difficulty:
  - Strategic risks are difficult to quantify and measure.
  - Strategic risks often manifest themselves over a longer period of time than managers are accustomed to evaluating.
  - Assessing strategic risks requires managers to think about the downside of the business strategies that they are naturally optimistic about *("negative risk is perceived to be a third-party phenomenon" – Jona Owitti)*
  - Strategic risks often arise out of significant uncertainty and can be unprecedented. Leaders must expend additional effort in order to identify and monitor potential strategic risks.

65

Enterprise Risk Management
ERM in Strategy-Setting

Protiviti's method (called a "contrarian approach") to risk assessment is premised on the following:

- The success of every business strategy hinges on a set of assumptions about factors like:
  - the state of the business environment,
  - competition, and/or
  - the operational capability of the organisation to execute the strategy.
- The contrarian approach connects strategy-setting and risk assessment by identifying the assumptions underlying each business strategy and then asking:
  - "What if these assumptions turn out to be wrong?"

66

Enterprise Risk Management
ERM in Strategy-Setting

The steps to Protiviti's approach include the following:

- Identify the most important assumptions underlying a particular strategy.
- Articulate statements that contradict these assumptions. Since an assumption represents a positive condition necessary to the success of a strategy, the contradiction is the negative impact.
- Brainstorm various scenarios that could create the negative conditions captured in the contrarian statements.
- Rate the risk scenarios based on criteria such as the impact of the scenario on the organisation.
- Develop a response to the identified strategic risk scenarios, and also develop methods for monitoring risks as they develop
  (Monitoring risks can be aided by tools like key risk indicators (KRIs))

67

Enterprise Risk Management

PAUSE

– Next Slides –

Role of Audit Committees in Risk Oversight

68

Enterprise Risk Management
Role of Audit Committees in Risk Oversight

Audit Committee Responsibility:

- Responsible to the board for:
  - oversight of management reporting on internal control
  - the internal auditors play a key role in assessing and reporting on risk management and internal controls

  Hence, the two entities above share a healthy interdependence.

69

Enterprise Risk Management
Role of Audit Committees in Risk Oversight

Audit Committee Responsibility:

- To provide adequate oversight of internal auditing, an audit committee should ensure, among others, that:
  - It (the audit committee) has a clear understanding of the strengths and weaknesses of the organisation's internal control and risk management systems.

70

Corporate Governance & Risk Management

Concluding Remarks

71

Enterprise Risk Management

(Current Issues and Risk Management)

Issues:

- Increasing regulatory and private scrutiny
- Risk is an essential part of any business
- Drives growth and opportunity (if properly managed)
- Business pressures (a struggle for executives) – e.g.,
  - Distressed financial markets
  - Mergers
  - Acquisitions
  - Restructuring
  - Disruptive technology change
  - Geopolitical instabilities
  - Rising price of energy

72

Enterprise Risk Management

(Current Issues and Risk Management)

Consider Impact of technology and regulatory requirements:

- Changing operating environment (business)
  - Use of and reliance on technology
  - Demand for "timely" information
  - Manual to online / real-time environment
  - "Act Electronic" but "Think Manual"
  - The "I-family" (I-pad, I-pod, I-phone, I-everything)
  - Cloud Computing
- Regulatory requirements and responsibilities
  - e.g., Sarbanes/Oxley Act (SOX) Section 404 on financial reporting requires publicly-quoted corporations to utilize a control framework in their internal control assessments – e.g., COSO; Consider Kenya's regulatory requirements on RM
  - Can delegate 'performance' but not 'responsibility'

73

Thank You

Q & A

Jona Owitti, CISA:
Membership Director, ISACA Kenya Chapter
and
Director, Security Risk Solutions Ltd

E-mail address: jona.owitti@yahoo.com;
jona.owitti@securityrisksolutions.net
Website: www.securityrisk-solutions.com

74