Enterprise Risk Management
Sources . Universe . Tolerance . Appetite

Presentation Made at the ICPAK ERM Conference
Wednesday, 20th March 2013
Hilton Hotel, Nairobi – 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)*

"Risk is like fire: If controlled it will help you; if uncontrolled it will rise up and destroy you."
Theodore Roosevelt

1

Enterprise Risk Management

About the Presenter: Jona Owitti, CISA

Specialisation / Interest: Information Systems (IS) Auditing, Information Security; Risk and IT Governance
Presenter at: National (e.g., ICPAK, IIA) and International (e.g., MISTI)
Now: Security Risk Solutions Ltd – Director, Government & Public Sector
Membership Director – 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); 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

Enterprise Risk Management

Agenda / Coverage

- Introduction to Enterprise Risk Management (ERM)
  - Terms, Definitions and Principles
- Sources of Risk and Risk Universe
- Risk Tolerance and Risk Appetite
- Conclusion, Discussion / Q&A

3

Enterprise Risk Management

Introduction to Risk Management

Overview / Definitions / Principles

4

Enterprise 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".

5

Enterprise 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.

6

Enterprise 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.

7

Enterprise 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.

8

Enterprise 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.

9

Enterprise Risk Management
(Why is ERM 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)

10

Enterprise 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

11

Enterprise Risk Management

PAUSE

– Introduction Summary –

(COSO ERM Cube)

12

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

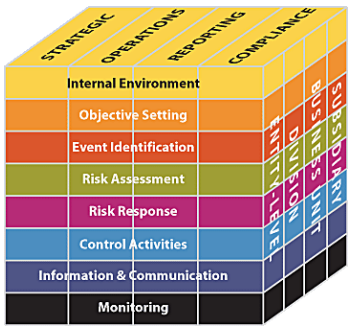
(See ERM Cube below for COSO depiction)

13

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)

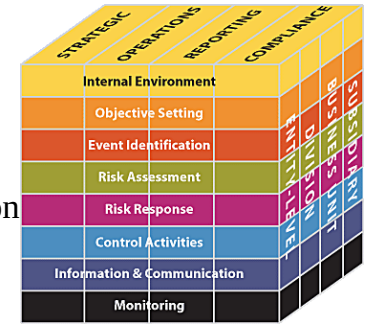
14

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
- Control Activities
- Information & Communication
- Monitoring

(Source: COSO)



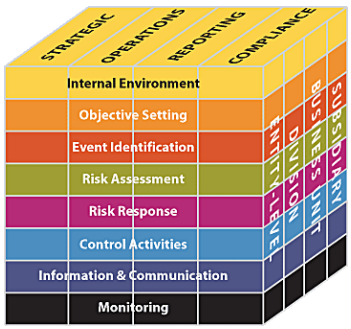
15

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)



16

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'.

17

Enterprise Risk Management

Strategic Planning for Risk Management

- RM involves choosing alternatives that can:
  - reduce risk within the operation, or
  - transfer risk outside the operation, or
  - increase the operations ability to bear risk
- No single strategic plan for RM will work for everyone because:
  - risk attitudes are different,
  - business goals are different, and
  - the resource base is different

18

Enterprise Risk Management

PAUSE

– Next Slides –

Sources of Risk and Risk Universe

19

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]

20

Enterprise Risk Management
Sources of Risk

Notes:

- Sources of risk may depend on the industry / sector being considered:
  - Banking / Financial
  - Agricultural
  - Energy
  - Utility
  - Health
  - etc
- Not everyone views the same set of circumstances as being equally risky. Some people are naturally more optimistic, while others are always looking for the worst possible outcome to happen.

21

Enterprise Risk Management
Sources of Risk

Notes *(cont'd)***:**

- Everyone must decide for themselves what levels of risk they are comfortable living with.
- Hence, everyone needs to be actively engaged in the management of the operation of their organisations.
- Risk and return are inseparable concepts.

22

Enterprise Risk Management
Sources of Risk

Sources of Risk:

- External Risks

- Internal Risks

23

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

24

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)

25

Enterprise Risk Management
Sources of Risk

Sources of Risk: Examples

26

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.

27

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

28

Enterprise Risk Management

PAUSE

– Next Slides –

Sources of Risk and Risk Universe

29

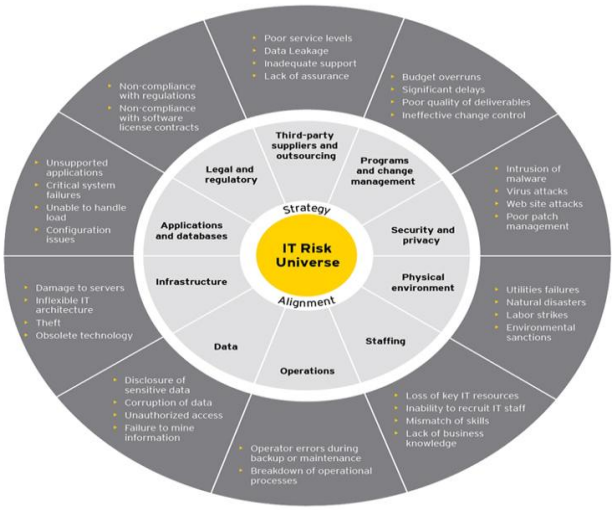
Enterprise Risk Management
Risk Universe

Risk Universe (Definition):

- All risks that could affect an entity.
- The full range of risks which could impact, either positively or negatively, on the ability of the organisation to achieve its long term objectives.
- Analogy: Consider “Audit Universe”

30

Enterprise Risk Management
Risk Universe: IT Risk Universe Example
(Source: ISACA)



Enterprise Risk Management

PAUSE

– Next Slides –

Risk Appetite and Risk Tolerance

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, 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.

33

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 customer "

34

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

35

Enterprise Risk Management
Designing a Risk Appetite

(Source: The Institute of Risk Management (Risk Appetite & Tolerance Guidance Paper (2011))

Questions to Ask, include:

- Has the board and management team reviewed the capabilities of the organisation to manage the risks that it faces?
- What capacity does the organisation have in terms of its ability to manage risks? Are there any particular issues of which the board should be aware? How mature is risk management in the organisation? Is the view consistent at differing levels of the organisation? Is the answer to these questions based on evidence or speculation?
- What specific factors should the risk appetite take into account in terms of the business context? Risk Processes? Risk Systems? Risk management maturity?

36

Enterprise Risk Management
Designing a Risk Appetite

(Source: The Institute of Risk Management (Risk Appetite & Tolerance Guidance Paper (2011))

Questions to Ask, include (cont'd):

- At which levels would it be appropriate for the board to consider risk appetite?
- What are the main features of the organisations risk culture in terms of tone at the top? Governance? Competency? Decision making?
- How much does the organisation spend on risk management each year? How much does it need to spend?
- Does an understanding of risk permeate the organisation and its culture?
- Does each individual understand their role and responsibility for managing risk?

37

Enterprise Risk Management
Designing a Risk Appetite

(Source: The Institute of Risk Management (Risk Appetite & Tolerance Guidance Paper (2011))

Questions to Ask, include (cont'd):

- At a managerial level, do you know what level of risk you should take? Do you know who the risk owners are? Do they have systems in place for measuring and monitoring risk?
- Is management incentivised for good risk management?

38

Enterprise Risk Management

Concluding Remarks

39

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 org. executives) – e.g.,
  - Distressed financial markets
  - Mergers
  - Acquisitions
  - Restructuring
  - Disruptive technology change
  - Geopolitical instabilities
  - Rising price of energy

40

Enterprise Risk Management

(Current Issues and Risk Management)

Consider Impact of technology and regulatory requirements on RU, RA & RT):

- 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
  - Can delegate 'performance' but not 'responsibility'

41

Enterprise Risk Management

Q&A / Discussion

42

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

43