Enhancing Third-Party Risk Management

Thursday, 12th September 2019

Presentation by:
CPA Timothy Kimathi
Director & Principal Consultant
Management Audit Consulting Ltd

CONTENTS

- *Overview of TPRM Model*
- *Overcoming challenges in TPRM*
- *Role of Internal audit in TPRM*
- *Case Study?*

Some definitions ....

Risk Management is a structured, consistent and continuous process for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of an entity's objectives.

Some definitions ....

Third Party Risks are those risks associated with third parties with which an entity does business and/or shares data with (suppliers, service providers, agents, joint ventures, etc.)

Hence Third-Party Risk Management can be described as the process through which an entity seeks to understand those risks, analyze, and mitigate them. Ideally, it should be an element of the larger ERM framework of the entity.

Types of TPRs ....

- Risks associated with third parties

Source: E&Y

TPRs may include ....

- Operational risks – disruptions to your processes due to non-performance by TP
- Reputational risks – TP may engage in activity that adversely affects your reputation
- Legal & Regulatory – your organization can be found liable out of actions by TP
- Cyber risks – cyber criminals can gain access to your systems via TPs.
- Etc.

Why TPRs are increasing....

Historically, TPRs were mainly considered to be 'procurement' issues.

- Procurement identifies suitable supplier
- Legal prepares contract
- Execution of contract, with very little monitoring
- No consensus on who 'owns' TPRs

Why TPRs are increasing....

Changing business environment:

- Increased outsourcing – now on a global scale (outsourcing is a method of mitigating risk!)
- Technology
- Regulation
- Insufficient resources to manage TPRs.

Outsourcing ... Apple Inc

Outsourcing ... Apple Inc

Outsourcing ... Apple Inc

TPRM Model ....


Termination
Planning
Third Party Risk Management
Vendor Management
Due Diligence
Contracting

Overcoming challenges in TPRM

- **Planning**
- Consider need to engage TP (costs/benefit), then develop a sourcing strategy
- **Perform due diligence**
- Who are the shareholders of the TP entity (e.g. are they PEPs?); are there lawsuits against the company? negative media reports? financial capacity? does TP have BCP/DRP?

Overcoming challenges in TPRM

- On-site reviews – obtain certification by regulators, professional bodies, etc.
- References checks
- Identify specific risks associated with TPs, evaluate, and rank the risks.

Overcoming challenges in TPRM

❖ Selection/onboarding TPs

- ensure contracts are comprehensive
- include performance and compliance requirements

❖ Management

a) Oversight & Governance (ownership of TPRM, governance structure)

Overcoming challenges in TPRM

b) Identify TPs & the risks associated with them. Maintain a comprehensive inventory.

c) Assess the risks (likelihood, impact).

d) Rank/categorize the risks to help focus on the critical ones.

e) Develop and implement policies, procedures & controls to mitigate the risks

Overcoming challenges in TPRM

❖ Monitoring

- Perform contract compliance audits
- Regular reporting

❖ Termination

- On need-to basis
- Manage the termination process.

Risk Management responsibilities

The board delegates the responsibility for RM to Management. However, the board remains ultimately responsible.

The board, therefore, needs assurance that RM in the entity is working effectively.

Risk Management responsibilities

Assurance is obtained from:

- Management of the entity – periodic reports (effectiveness of the RM process, emerging risks, failures of control measures, etc.)
- Internal Auditors – who should provide *independent* & *objective assurance* on the effectiveness of the RM process
- Others – external auditors, etc.

IPPF Standards

Standard 2010 – Planning

The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

[Risks posed by an organization's third-party providers should be considered in the development of a comprehensive risk-based audit plan – *Practice Guide*].

IPPF Standards

Standard 2010 – Planning

In planning an engagement, the internal auditor considers the *significant risks of the activity* and the means by which management mitigates the risk to an acceptable level.

IPPF Standards

Standard 2120 – Risk Management

The internal audit activity *must* evaluate the effectiveness and contribute to the improvement of risk management processes.

The IA needs to ascertain whether:

- Organizational objectives support and align with the organization's mission;

IPPF Standards

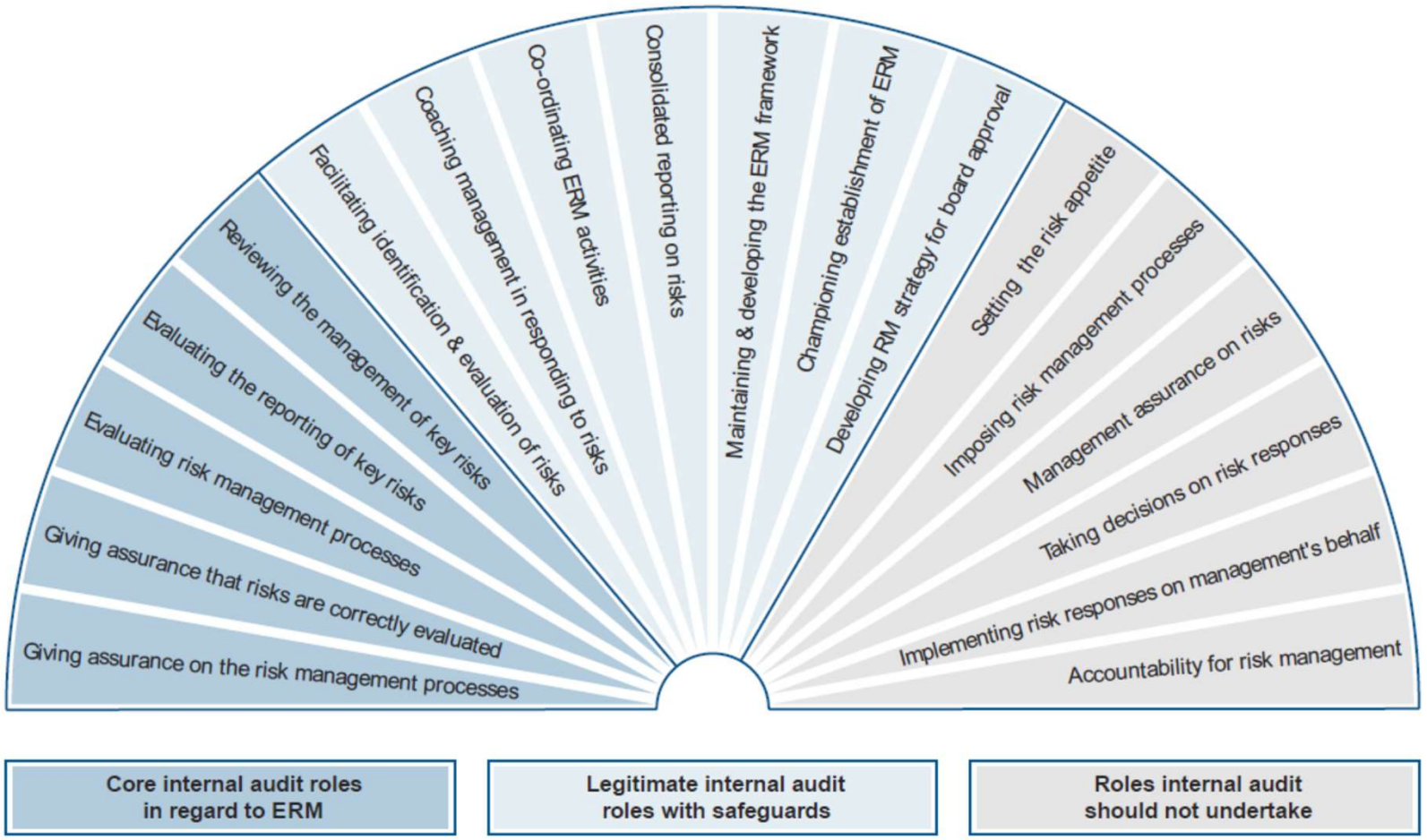
- Significant risks (including TPRs) are identified and assessed;
- Appropriate risk responses are selected that align risks with the organization's risk appetite; and
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

IIA Position Paper

Key factors to consider in performing RM roles:

- **Does the activity compromise the IA's independence and objectivity?**
- **Does the activity improve the entity's risk management, governance and control processes?**

Figure 1 – Internal audit role in ERM



- ***Source: IIA Position Paper – Role of Internal Audit in ERM***

IIA Position Paper

Internal auditors will normally provide assurances on three areas:

- Risk management processes, both their design and how well they are working;
- Management of those risks classified as 'key', including the effectiveness of the controls and other responses to them; and
- Reliable and appropriate assessment of risks and reporting of risk and control status.

IIA Position Paper

IA core roles in RM:

- Reviewing the management of key risks
- Evaluating the reporting of key risks
- Evaluating, and giving assurance on, the RM processes
- Giving assurance that risks are correctly evaluated

IIA Position Paper

IA roles with safeguards:

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

IIA Position Paper

Roles IA should not perform roles:

- Setting the risk appetite
- Imposing RM processes
- Providing assurance (on behalf of management) on risks
- Taking decisions on risk responses
- Implementing mitigations/controls on behalf of management
- Accountability for RM

IIA Position Paper

Safeguards:

- Management remains responsible for risk management.
- Nature of IA's responsibilities should be documented in the IA Charter.
- Any work beyond the assurance activities should be recognized as a consulting engagement and the implementation standards related to such engagements should be followed.

Case Study – Agri-based company

Nature of operations

- involves extensive use of manual labour to harvest the primary material used to produce the company's main product
- harvesting also involves use of sharp tools
- cost/benefit analysis done and decision made to outsource the harvesting operation to a third party

Case Study – Agri-based company

Risks associated with outsourcing to third party

- Product's main market is in Europe – a market sensitive
- Reputational risks due to, for example, unethical practices such as use of child labour, poor working conditions, etc.

Case Study – Agri-based company

Risk management

- Contractor signs contract stipulating the T&C
- Contractor must provide statutory docs such as ID to company's labour office to ensure underage persons are not engaged
- Company provides PPE directly to labour
- Regular OSHA audits by independent party
- Close inspections by senior company staff

Thank you!!

Management Audit Consulting Limited
Davard House, Cedar Road off Rhapta Road, Westlands
Tel: 4450890/1, 0715096708, 0736952271
Email: info@managementaudit.co.ke
Website: www.managementaudit.co.ke