ICPAK

PERFORMING AN ERM HEALTH CHECK

Presentation at the Enterprise Risk Management Seminar

Friday, 7th August 2015

Timothy Kimathi
Director - Management Audit Consulting Ltd

- Why ERM matters
- Effective ERM systems
- Assessing the ERM system

Why ERM matters

- No enterprise operates in a risk-free environment
- Some of the recent checkpoints that have driven the need for ERM
  - ✓ Greater uncertainty (globalization, security, technology)
  - ✓ Greater requirement for transparency/Good governance
  - ✓ Stronger Regulatory / Compliance Environment

Why ERM matters

ERM supports value creation by enabling management to:

- **Identify potential future events that can negatively impact the organization**
- **Respond in a manner that reduces the likelihood & impact of downside outcomes and exploits the upside**

Effective ERM Systems

1. Various guidelines exist, including:
   - COSO
   - ISO 31000
2. Process is largely similar, and comprises of key stages:
   - ❖ Internal environment
   - ❖ Objectives
   - ❖ Events identification
   - ❖ Risk assessment – likelihood & impact
   - ❖ Risk response – strategies to manage the risks
   - ❖ Controls to mitigate the risks
   - ❖ Information & communication
   - ❖ Monitoring & feedback

Status of ERM?

- **'ERM is happening whether you have a formal program or not. The issue is how well you're doing it' – Gary Bierc, CEO of rPM3 Solutions LLC**

Status of ERM?

- **Many organizations have some form of ERM framework; however, the level of ERM maturity differs**

- **According to an article by Deloitte:**

1. ***Initial stage***

- ❑ RM is ad hoc/chaotic
- ❑ No formal procedures for RM
- ❑ Very few risks are considered

Status of ERM?

2. Fragmented

- Risk is differently defined at different levels in the organization
- Silo management of risks; limited linkages
- Limited alignment to strategy

3. Comprehensive

- Risk universe is identified
- Common approach to assessment/response
- Risks are prioritized
- Strategic risks are communicated

Status of ERM?

4. Integrated

- Risk management activities are co-ordinated
- ERM monitoring, measuring and reporting
- Opportunities are identified and exploited
- Ongoing risk assessment process

5. Strategic

- Risk discussion is embedded in Strategic Planning, resource allocation, product development, etc.
- Early warning system to 'flag' risks above established threshold to Board & senior management

Performing the Health Check – who needs it?

Board of directors

Have oversight role to determine that appropriate risk management processes are in place and are adequate and effective

Executive Management & Business Process Owners

They 'own' the system and are responsible for developing, implementing, and monitoring ERM, and ensuring effective reporting to the Board

Performing the Health Check – who needs it?

Internal Auditors

IPPF standard 2120 – the IA activity ***must evaluate the effectiveness***…of the risk management process.

In other words it is a requirement to do an ERM health check – if IA are to comply with the IPPF!

Key factors to consider

1. Internal environment:

- Risk management philosophy/TAT – integrity, ethical values
- Risk appetite
- Organizational structure – with clearly defined reporting lines, authority/responsibilities

2. Objective setting:

- SO aligned to its vision/mission
- Other objectives in line with SO
- Risk tolerance

Key factors to consider

3. Event identification:

- Potential events from external & internal environments
- Event identification techniques – historical events, current situation
- Risk event 'drivers'

4. Risk assessment:

- Estimating likelihood & impact (qualitative & quantitative)
- Risk ranking

Key factors to consider

5. Response:

- Strategies adopted (control, transfer, avoid, accept)
- Need to consider risk from an entity-wide perspective

6. Control activities:

- Actual mitigations – (policies, procedures, controls) that bring risk likelihood/impact within tolerance
- Type of controls – preventive, detective, etc.
- Assignment of responsibility for control activity
- Timelines for implementation of new controls

Key factors to consider

7. Information and Communication:

- Sufficient info at all levels (to enable identification, assessment and response to risks)
- Reporting

8. Monitoring:

- Compliance – how assessed? (departmental and corporate levels RMC)
- Frequency of reporting?
- Independent assessment by IA
- Periodic reviews to capture emerging risks

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