Internal Auditing Fundamentals—The Role of Internal Audit in Risk Management and Reporting

Milangu Kampata

August 2015
AGENDA

- Objective
- Risk Management overview
- Role of Internal Audit in Risk Management
- Reporting on Risk Management
- Reflect
- Questions
OBJECTIVE

To clarify the role of internal audit in risk management and reporting.
Defining risk

- The IIA's International Standards define a risk as 'the possibility of an event occurring that will have an impact on the achievement of objectives.'
Risk can be either positive (or negative aspects)

- Potential benefits
- Adverse Impact

(upside risk) (downside risk)
Defining risk management

- Risk Management refers to the process used by an organisation to monitor and mitigate its exposure to risks. It includes identifying and assessing risks (the “inherent risks”) and then responding to them.

- Risk is measured in terms of impact and likelihood.

- Risk management is a fundamental element of corporate governance.
Defining Enterprise Risk Management (ERM)

Enterprise risk management (ERM) describes what happens when organisations put in place a structured, continuous process to identify, manage and respond to risk.
RISK MANAGEMENT OVERVIEW

Risk Management Process

Set Objectives

Identify risks to the achievement of objectives

Assess the impact and likelihood of risks

Evaluate risk priorities

Response to risks

Communicate consultation and coordination

Monitor, review and report on the effectiveness of risk treatment and actions
Definition of internal auditing

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations.

It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
About the definition of internal auditing

- The Definition of Internal Auditing is the statement of fundamental purpose, nature and scope of internal auditing.

- The definition is authoritative guidance for the internal audit profession from the Global Institute of Internal Auditors. It is part of the International Professional Practices Framework (IPPF).
Standard 1000 – Purpose, Authority, and Responsibility

- The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Definition of Internal Auditing, the Code of Ethics, and the Standards.

- The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.
The IIA issued a position paper on the role of internal auditing/assurance services with regards risk management and consulting role they may undertake depending on the risk maturity of the organisation.

It is expected that as the organisation's risk maturity increases and risk management becomes more embedded that internal audit's role in championing risk management is reduced.
WHAT SHOULD IA DO – RISK MGT

- Internal auditing can provide consulting services (e.g. tools to use, co-ordinate) so long as they have no role in actually managing risks - that is management responsibility.

- Tools – can provide tools like risk register templates for a standardized approach

- Co-ordinate – IAs understand risks & controls so can champion and assist management, however senior management must actively be involved, endorse & support ERM
Internal auditing is an independent objective assurance and consulting activity.

Its core role with regards to ERM is to provide assurance to the board on the effectiveness of risk management.
The principle that management is responsible for managing risks is clearly stated in many documents outlining best practices for governance and risk management.

This includes the Guidance on Internal Control (Turnbull) and the Guidance on Audit Committees (Smith) that are annexed to the Financial Reporting Council’s Code of Corporate Governance and also the Good Governance Standard for Public Services published in 2005 by the Independent Commission on Good Governance in Public Services, established by the Office for Public Management (OPM®) and the Chartered Institute of Public Finance and Accountancy (CIPFA).
ROLE OF IA IN RISK MANAGEMENT

- Internal Audit is not responsible for the organisation’s risk management.
- The internal auditor should never assume any management responsibility for risk and should avoid being involved in any risk management activities that might compromise their independence or objectivity.
- Prohibiting internal audit from having operational responsibility or authority over areas audited.
REPORTING ON RISK MANAGEMENT

Two ways that Internal Auditing provides value to orgn.

- Providing objective assurance that the major business risks are being managed appropriately
- Providing assurance that the risk management & internal control framework is operating effectively.
## Reporting on Risk Management

<table>
<thead>
<tr>
<th>Risk Maturity</th>
<th>Key Characteristics</th>
<th>IA Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Naïve</td>
<td>No formal approach developed for Risk Management</td>
<td>Promote Risk Management and rely on audit risk assessment.</td>
</tr>
<tr>
<td>Risk Aware</td>
<td>Scattered silo based approach to risk management</td>
<td>Promote Risk Management and rely on audit risk assessment.</td>
</tr>
<tr>
<td>Risk Defined</td>
<td>Strategy and policies in place and communicated. Risk appetite is defined.</td>
<td>Facilitate risk management and use management’s assessment of risk as appropriate.</td>
</tr>
<tr>
<td>Risk Managed</td>
<td>Enterprise-wide approach to risk management developed and communicated</td>
<td>Audit risk management process and use management’s assessment of risk as appropriate.</td>
</tr>
<tr>
<td>Risk Enabled</td>
<td>Risk Management &amp; internal control embedded in operations.</td>
<td>Audit risk management process and use management’s assessment of risk as appropriate.</td>
</tr>
</tbody>
</table>
REPORTING ON RISK MANAGEMENT

<table>
<thead>
<tr>
<th>Risk Maturity Stage</th>
<th>Guide - IA Reporting on Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Risk Naïve</td>
<td>• Report that no formal risk management</td>
</tr>
<tr>
<td></td>
<td>• Assurance on control processes</td>
</tr>
<tr>
<td>• Risk Aware</td>
<td>• Report poor risk management</td>
</tr>
<tr>
<td></td>
<td>• Assurance on control processes</td>
</tr>
<tr>
<td>• Risk Defined</td>
<td>• Report risk management deficiencies</td>
</tr>
<tr>
<td></td>
<td>• Assurance on risk management policies</td>
</tr>
<tr>
<td></td>
<td>&amp; on control processes</td>
</tr>
<tr>
<td>• Risk Managed</td>
<td>• Assurance on risk management processes</td>
</tr>
<tr>
<td></td>
<td>&amp; mitigation</td>
</tr>
<tr>
<td>• Risk Enabled</td>
<td>• Assurance on risk management processes</td>
</tr>
<tr>
<td></td>
<td>&amp; mitigation</td>
</tr>
</tbody>
</table>
Report your conclusion on risk maturity to management and to the audit committee.

This stage will provide a first, high level, assurance on the risk management processes, the management of key risks and on the recording and reporting of risks.
Assurance Mapping exercise involves mapping assurance coverage against the key risks in an org.

This allows an org to identify and address any gaps in the risk mgt process & gives stakeholders comfort that risks are being managed & reported on, and that regulatory & legal obligations are being met.
IA provide assurance that:-

• management’s risk management processes to identify, evaluate, monitor and report on risk are operating effectively

• the response is operating effectively
IA provide assurance over the entire orgn

• Risk mgt processes (both design & operating effectiveness)

• Management of those risks classified as key (including effectiveness of the controls and other responses to them),

• Verification of the reliability and appropriateness of the risk assessment

• Reporting on risk & control
RBIA also provides assurance that management’s risk management processes to identify, evaluate, monitor and report on risk are operating effectively.

RBIA provides assurance that the response is operating effectively e.g. response by management may be:

- Tolerate - do nothing
- Transfer - pass the risk to another party
- Treat – implement a system of internal control to reduce the risk
- Terminate - remove the circumstances giving rise to the risk.
- Take opportunity
Where are you in our organisations with regards RM and your roles as IA?
If answer is Yes
• Managing risk?
• Objective threatened?
• Independence threatened?

Then Internal Auditors must

If answer is NO
• Provide assurance
Any Questions?