INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS OF UGANDA

THE ROLE OF INTERNAL AUDIT IN RISK MANAGEMENT

OCTOBER 2024

Plot 42 Bukoto Street, Kololo, P.O. Box 12464, Kampala, UGANDA
Tel: 041-4540125
standards@icpau.co.ug
www.icpau.co.ug

TABLE OF CONTENTS

ABOUT ICPAU

The Institute of Certified Public Accountants of Uganda (ICPAU) was established under the Accountants Act, Cap 294.

The functions of the Institute as prescribed by the Act are to:

i) Regulate and maintain the Standard of Accountancy in Uganda and

ii) Prescribe and regulate the conduct of accountants and practicing accountants in Uganda.

Under its legal mandate, the Institute prescribes professional standards to be applied in the preparation and auditing of financial reports in Uganda.

Vision

A globally recognized promoter of accountants for sustainable economies.

Mission

To develop and regulate accountants for professional excellence and sustainable impact.

Core Values

1) Professional Excellence
2) Accountability
3) Integrity
4) Responsiveness

International Affiliations

The Institute is a member of the International Federation of Accountants (IFAC) and the Pan African Federation of Accountants (PAFA).

DISCLAIMER

This paper is prepared to create awareness about the role of internal auditors in the risk management processes of their organizations.

ICPAU disclaims any responsibility or liability that may occur, directly or indirectly, as a consequence of the use and application of this Guide.

1.0 INTRODUCTION

Risk is defined by the Committee of Sponsoring Organisations of the Treadway Commission (COSO) as the possibility that events will occur and affect the achievement of strategy and business objectives. The world is rapidly changing which implies that many businesses today are grappling with emerging risks associated with these changes. This means that agile organizations need to have robust risk management processes to ensure all risk exposures are managed at acceptable levels. This Paper highlights the role of internal auditors in the risk management process.

2.0 THE RISK MANAGEMENT PROCESS

Risk management is the structured, consistent, and continuous process across the organization for identifying, assessing, deciding on responses to, and reporting on opportunities and threats that affect the achievement of organizational objectives[1]. Effective risk management processes, therefore are composed of the following steps for management, analysis, prioritization, and monitoring of risks.

2.1 Risk Identification

The risk management process begins with the establishment of the context through which organizational objectives are well stated and how risks are evaluated. During this stage, all potential risks that could derail the achievement of organisational objectives are identified. This requires good knowledge of the business as well as the industry's market including the legal, social, economic and political environment.

2.2 Risk Analysis and Assessment

After the risks are identified, they need to be assessed on the basis of their severity and likelihood of occurrence. Risk assessment should ideally be done at least annually and risks should be logged in a risk register or risk inventory that describes the risk, the likelihood that the risk will be realised (likelihood/ probability), the impact if the risk is realised, the plan and time period for mitigating the risk and the person responsible for that risk.

2.3 Risk Treatment

Once risks are identified and assessed, appropriate techniques are then identified to manage the risks to an acceptable level. Overall, depending on the severity and likelihood of occurrence, risk management strategies are categorized in the following categories:

[1] IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management

a) Risk transfer – This strategy involves the transfer of all or part of the losses consequential to the risk exposure to another party (usually an insurance company), at a cost.

b) Risk avoidance – This strategy involves the avoidance of risks or circumstances that may lead to losses. In so doing, the risk of reduced earnings is enhanced as this strategy reduces the possibility of earning profits from the avoided circumstances or strategies.

c) Risk retention – This strategy involves the retention of losses due to risks. The losses are assumed by the organisation as acceptable losses in the normal course of its operations. This strategy is largely dependent on the organisation's risk appetite (the level of risk that an organisation is willing to accept).

d) Risk reduction – This strategy involves the reduction of losses associated with the identified risks through preventative measures.

2.4 Risk Monitoring and Review

Risk analysis and management plans should be updated regularly to evaluate their effectiveness in light of the changing business environment. This stage, therefore involves continuously updating the risk register to ensure that all emerging risks are addressed and that the proposed risk management strategies are effective. The reviews may be done through internal control processes such as supervisory reviews, transaction reviews and performance metrics or through a combination of internal and external assessments from internal and external auditing exercises.

3.0 THE THREE LINES MODEL

Organizations are often operated with multiple stakeholders with diverse and sometimes competing interests. Because of this, organizations need effective structures and processes to enable them to achieve their organizational objectives while supporting strong governance and risk management. The Three Lines Model helps organizations identify structures and processes to achieve strong governance and risk management.

The Three Lines Model is a valuable framework that outlines the internal audit's role in risk management and good corporate governance. According to the Model, different levels of an organization play different roles in risk management as indicated below:

a) The First Line of Defence

This level is comprised of management and staff who are responsible for the identification and management of risks as part of their accountability for the achievement of objectives.

b) The Second Line of Defence

This level is comprised of functions that oversee or specialize in compliance or risk management. These functions typically provide the policies, frameworks, tools, techniques, and support to enable risk and compliance to be managed by the first line. These functions also conduct monitoring of the established policies and processes to ensure their effectiveness. Therefore, the second-line roles include monitoring, providing advice and guidance, testing, analysing, and reporting on matters related to the management of risk.

c) The Third Line of Defence

This level is comprised of functions that provide independent assurance. The main role of the functions on the third line is to ensure that the first two lines are operating effectively and advise how they could be improved. This is best performed when the internal auditing function is independent of management.

Internal audit functions should be set apart from other functions to enhance their independence and distinctive value in assurance and advisory services. In situations where this level of independence cannot be achieved, it is more prudent that the internal auditing function be provided by a qualified third party.

4.0 INTERNAL AUDIT ROLE IN RISK MANAGEMENT

Internal audit functions as part of the third line of defense, providing independent and objective assurance and advice on the adequacy and effectiveness of governance and risk management processes. Those charged with governance require assurance that risk management processes are working effectively and that key risks are being managed to an acceptable level. While this assurance may come from different sources, the internal audit function is a key source. Some of the specific roles of internal audit in risk management include providing:

a) Objective assurance that the risk management and internal control systems are operating effectively. This role requires internal auditors to undertake activities such as:
   i) Facilitating the identification and evaluation of risks and providing assurance that risks are correctly evaluated.
   ii) Providing assurance that the risk management processes adequately address the key risks
   iii) Providing a consulting role in the establishment of risk management frameworks.

b) Consulting services that improve an organization's governance, risk management, and control processes. This role varies from time to time and is dependent on other

factors such as the available resources and the risk appetite of the organization. Some of the consulting roles that internal auditing may undertake in relation to risk management include:

i) Making available to management tools and techniques used by internal audit to analyse risks and controls;
ii) Being a champion for the introduction of risk management in organizations,
iii) Provision of advice, facilitating workshops, and coaching organizations on risk management;
iv) Acting as a central point for the coordination, monitoring, and reporting of risks; and
v) Supporting management to establish the best ways of mitigating risks.

Great care should be taken while acting in a consulting capacity for internal auditors not to assume any management responsibility. The establishment and management of risk management processes remain management responsibility. Therefore, internal auditors should restrict themselves to supporting management in achieving this without taking over management's full responsibility.

5.0 CONCLUSION

Risk management is a fundamental component of corporate governance. Those charged with governance should establish robust risk management processes to mitigate risk exposure. The internal audit's role can be summarized as providing assurance on the effectiveness of the risk management processes in their organizations.