INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS OF UGANDA

THIRD-PARTY RISK MANAGEMENT

FEBRUARY 2024

Plot 42 Bukoto Street, Kololo, P.O. Box 12464, Kampala, UGANDA
Tel: 041-4540125, 0393-262-333, 0393-265-590
standards@icpau.co.ug
www.icpau.co.ug

TABLE OF CONTENTS

ABOUT ICPAU

The Institute of Certified Public Accountants of Uganda (ICPAU) was established in 1992 by the Accountants Act, Cap 266. This has now been repealed and replaced by the Accountants Act, 2013.

The functions of the Institute as prescribed by the Act are to regulate and maintain the Standard of Accountancy in Uganda and to prescribe and regulate the conduct of accountants and practising 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 recognised 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 raise awareness about third party risks and to guide internal auditors to become trusted business advisors to their organisations especially in regards to third party risk management.

Internal auditors may utilize the paper in light of their professional judgment and the facts and circumstances involved in their organisations and each particular engagement.

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

Entities today are increasingly relying on third parties in different ways to deliver products and services or outrightly outsourcing some of their critical business functions. However, this leaves such entities exposed to various third-party risks such as data breaches, regulatory non-compliance, operational disruptions, reputational damage and legal liabilities. This paper is prepared to publicise the risks brought to entities through interactions with external parties and to guide internal auditors while assuring third-party risks.

2.0 THIRD PARTY RISKS EXPLAINED

A third-party risk is any risk exposure that an entity faces due to interactions or business relationships with external parties such as vendors, suppliers, business partners, or service providers. The frequent dealings with external parties enable such parties to gain access to internal entity or customer data, systems, processes, and other privileged information. This eventually leaves the concerned entity exposed to risks such as:

a) Cybersecurity risk: the risk of exposure or loss resulting from cyber-attacks and data breaches.

b) Operational risk: the risk that a third party will disrupt the business operations. These risks impact the entity's ability to meet customer demands or achieve the desired strategic objectives. This is especially common for financial institutions.

c) Legal, regulatory, and compliance risk: the risk of penalties due to the failure by a third party to comply with relevant agreements, industry standards, or laws and regulations.

d) Reputational risk: the risk arising from negative perceptions caused by the actions or inactions of a third party such as poor performance or unethical behaviour.

e) Financial risk: the risk that a third party will have a detrimental impact on the financial performance of an entity for example, contractual breaches by the third parties leading to operational disruptions and eventually loss of revenue by the entity.

Third-party risks tend to be interlinked, for example, if an entity experiences cybersecurity breaches leaving customer data compromised, then it will most likely be exposed to financial, reputational, operational and compliance risks as well. Entities need to manage these risks effectively to ensure that they do not disrupt their business operations, reputation or result in legal and regulatory penalties.

3.0 THIRD PARTY RISK MANAGEMENT FRAMEWORKS

Third party risk management frameworks act as guides in the establishment of third-party risk management programs. While no single framework is likely to provide a comprehensive coverage to all third-party risks, entities are encouraged to draw inspiration from multiple third-party risk management frameworks when drawing up their third-party risk management systems. While there are several frameworks available, the commonly used frameworks are the Information Security Management System Standard (ISO), the Standardised Information Gathering Assessments (SIG), and the Security and Privacy Controls for Information Systems and Organisations (NIST). The choice of a third-party risk management framework should be based on the entity's structures and risk profile. An effective third-party risk management should include the following components:

a) Identification

This involves identifying the third parties that a particular entity works with and categorizing them based on the level of the risk they pose. This implies a review of third-party service contracts and agreements and the conducting of assessments or audits of third-party operations and systems.

b) Assessment

Evaluation of the risks associated with each third party, taking into account factors such as the type of services or products provided, the volume and sensitivity of data exchanged, and the location of the third-party operations.

c) Mitigation

Implementing controls such as security and compliance requirements, incident response plans and ongoing monitoring and reporting to mitigate the risks identified during the assessment phase.

d) Monitoring

Ongoing monitoring of third-party activities and performance including regular assessments and audits to ensure the effectiveness of the controls in the management of the third-party risks.

e) Reporting

Regularly reporting on the status of third-party relationships including any issues or incidents that have occurred and the actions taken to address them.

It's these components that eventually form the basis of the entity's third-party risk management programs.

4.0 CONSIDERATION OF ANTI-MONEY LAUNDERING IN THIRD-PARTY RISK MANAGEMENT

The global trends dictate that entities should comply with several rules and regulations to mitigate their exposure to money laundering risks and other financial crimes. Under the Financial Action Task Force (FATF) recommendations, entities must implement controls to manage the money laundering threats they face. This requires enhanced due diligence measures for third parties, a process of vetting, validating and verifying third parties prior to initiating a business relationship. This due diligence process is aimed at collection, analysis and evaluation of information that can be used to inform third party money laundering risk assessments. Such information includes:

- Entity names, addresses and incorporation documents
- Names and profiles of entity owners and directors
- Entity financial performance
- Debts, liabilities and other contingencies
- Internal business risk assessments and growth projections
- Historical anti money laundering compliance performance

The third-party risk management system in any entity should have the ability of giving assurance that the contracted third parties are not involved in criminal activities such as fraud, money laundering or financing of terrorism activities and that they are generally compliant with the AML/CFT regulations within their jurisdiction of operation.

5.0 ROLE OF INTERNAL AUDIT IN THIRD PARTY RISK MANAGEMENT

While the responsibility for managing third-party risks ultimately rests with management and those charged with governance, internal audit as the third line of defence has a role to play in assuring that the third-party risks to which the organization is exposed are addressed effectively. The role of internal auditors in third-party risk management can be manifested in the following ways:

a) Review of third-party controls and policies

Internal auditors need to provide assurance that all the third-party risk management systems as well as the third-party policies and procedures are aligned with third-party risks. This will require internal auditors to provide oversight around the third-party cycle, right from the sourcing stage to the issue resolution and termination stages. Some of the key activities involved are likely to be:

- Review of controls and policies as well as third-party risk assessment mechanisms to ensure that all the third-party risks that the organization is exposed to are catered for.

- Conduct additional research to understand the third parties employed by the organization and how engaging these third parties fits in the overall strategy of the organization.
- Review the third-party selection process to ensure third-party risk exposure is minimized through thorough due diligence.

b) Third-party risk assessment

Internal auditors support their organizations in the identification and assessment of risks associated with each of the third-party vendors that their entity deals with. This may involve assessing the significance of the risks identified by management as well as those identified during previous audit engagements or assessments of external parties or consultants.

Internal auditors also need to assess the effectiveness of their entity's third-party risk management systems to ensure that all third-party risks are accounted for.

c) Assurance over management's understanding of the compliance of third-party entities with relevant regulations or policies.

During the execution of their duties, internal auditors ought to perform procedures to enable them gain an understanding of third-party compliance with relevant laws and policies. This may necessitate selecting a sample of contracted third-party entities and evaluating whether both the organisation and these contracted entities adhere to relevant regulations and policies. This evaluation can be performed through verification of due diligence documentation, contractual compliance and monitoring activities.

d) Assurance over third-party monitoring processes

The role of internal audit can also be manifest in the provision of assurance over the effectiveness of the systems used by organisations to track third party relationships and interactions. This will necessitate the internal auditors' review of all the avenues through which organisations track third party relationships and how information regarding performance of the third parties is utilised in the general management of third-parties.

e) Issue resolution assessment

Internal auditors have a crucial role to play in providing assurance over how third-party issues are resolved. Internal auditors ought to report on the effectiveness of their organization's third-party risk management systems in ensuring that all concerns regarding third-party risk exposures, performance, quality of products or services, and any other issues that may be highlighted by the customers are addressed promptly.

f) Contract termination

In order to minimize the threat of litigation, internal audit may offer advisory services at third party contract termination stage to ensure that termination conditions in each contract are fulfilled by all the parties concerned.

6.0 PERFORMANCE OF THIRD-PARTY RISK ASSESSMENT

Like any other internal audit engagement, third-party engagements should start with engagement planning. During this stage, internal auditors should gather adequate information to enable them to understand third-party-related risks. This would necessitate internal auditors to:

- identify the various third parties engaged by the organization
- Review of existing third-party risk management frameworks. In circumstances where the entity being reviewed lacks such a framework, then the engagement will involve supporting the implementation of a third-party risk management framework.
- Review the level of documentation available for third-party risk management roles, responsibilities, and activities across the organization.
- Understand past issues encountered with third parties in terms of contracts, performance, and quality

Once the third-party risks have been identified, they should then be profiled using a risk matrix to ensure that the most impactful risks are addressed first. This is because the scarcity of resources in many entities implies a limitation in dealing with all the risks at ago. Therefore, the risks are profiled and handled periodically based on how impactful they have been rated to be.

With the risks identified, the third-party audit engagements can then be planned and executed with the major objective being to provide independent assurance over the governance, policies, processes, and key controls that support the implementation, execution, and oversight of the third-party risk management framework and processes[1]. This may be achieved through:

- Auditing of the third-party risk management framework and processes;
- Auditing of components of the third-party risk processes;
- Inclusion of third-party risk management in a process, product or unit audit.

Audits of third-party risk management require a different skillset from auditing traditional areas such as financial statements. Therefore, in conformance with Standard

[1] IIA Supplemental Guidance Practice Guide: Auditing Third-Party Risk Management

2230- Engagement Resource Allocation, the Chief Audit Executive should assess the skills of internal audit team members periodically to ensure that they have appropriate skills to evaluate the third-party risk management processes of the entity.

7.0 CONCLUSION

As organizations continually engage third-party entities, there is a need for well-established third-party risk management systems to proactively manage any third-party risks to which they may be exposed. The Internal audit function has a clear opportunity to help entities better understand and mitigate third-party risk. Therefore, every entity should ensure that internal audit is well positioned and supported to act as a key partner in third-party risk management efforts. For organizations that may not have fully fledged internal audit functions, those charged with governance in such organizations will ultimately remain responsible for managing risks associated with third-party relationships. To that effect, this paper may accord the necessary support and guidance to managing third-party risks for those charged with governance in such organizations.