FMM 05.8 Risked-Based Auditing

8.1 Introduction

Traditionally, internal audits focused on checking compliance with policies and procedures, often using a cyclical approach where every unit or process was audited at a set interval/frequency.

While compliance remains important, modern internal audit functions are increasingly risk-based. This shift ensures priority is given to areas where the agency is most exposed to negative outcomes—financial loss, fraud, reputational damage, or service delivery failures.

A risk-based approach focuses the audit plan and resources on the highest-risk activities, meaning those that could significantly impact the agency's mission or integrity if not well-controlled.

8.1.1 Why Risk-Based Auditing Matters?

By identifying and ranking risks, internal audit ensures that critical vulnerabilities receive prompt attention.

It also recognises, especially in PNG's fiscally constrained environment, that time and budget are limited. A risk-based plan allocates audit resources where they yield the greatest benefit—no wasted effort on low-risk, low-impact areas.

Agency leadership (including the Audit Committee) gain insights into top risks and receives targeted recommendations to strengthen controls and also encourages ongoing risk assessment, adapting as the agency's environment changes.

In more modern organisations it is common to merge the risk and audit functions together and form Risk and Audit Committees.

8.2 Mandated Policy

1. **All agencies are directed to adopt a risk-based approach in formulating their annual internal audit plans. The Department of Finance, through the**

PFMA and relevant sections of the Finance Management Manual, will supervise and guide agencies to ensure this method is consistently applied.

8.3 Non-mandatory Guidance

8.3.1 Authority and Prescribed Requirements

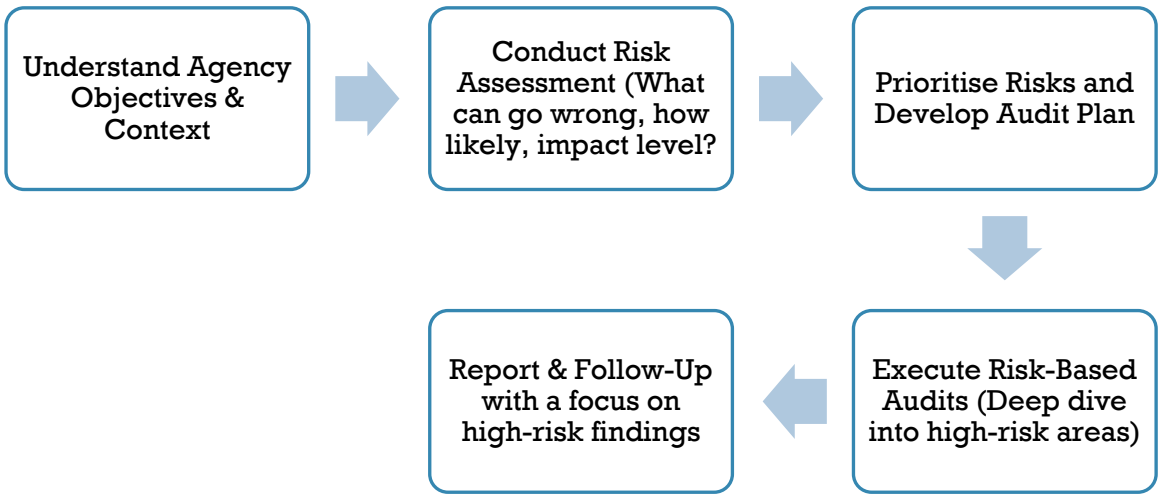
- Public Finances (Management) Act 1995 (PFMA) emphasises responsible use of public funds, implying that agencies should regularly assess and address areas posing significant risks to financial integrity.
- FMM Volume 2 sets out governance and accountability principles that require an understanding of operational and financial risks.
- IIA IPPF:
    - Standard 2010 (Planning) states: "The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity..."
    - Standard 2120 (Risk Management) underscores the internal audit's role in evaluating risk exposures and risk management processes.
- INTOSAI Guidance: INTOSAI's GOV 9140 on "Internal Audit Independence in the Public Sector" and related documents highlight the need for risk-focused audits to enhance accountability and transparency in government entities.

8.3.2 Understanding Risk-Based Auditing vs. Traditional Approaches

The following table simply summarises the differences between traditional and risk-based auditing:

Traditional (compliance-focussed)	**Risk-based**
Audits every unit/process on a fixed cycle	Audits areas based on priority of risk and impact.
Checklist-driven; often uniform scope.	Scope tailored to the specific risk profile.
Heavy emphasis on policy compliance.	Emphasises risk identification, mitigation, and strategic alignment.
May overlook emerging risks if not on the cycle.	Agile approach; adapts to new/emerging risks.
Often treats all findings as equally urgent.	Findings prioritised by potential impact and likelihood.

Much like the designing of internal controls, risk-based auditing starts with an identification of risks and below is a simplified diagram showing how risk-based auditing fits into an agency's audit cycle:



8.3.3 Understand Agency Objectives & Context

This requires a review of the agency's mandate (e.g., delivering health services, maintaining roads) and strategic priorities. It also requires the identification of laws, regulations, and policies that frame operations (e.g., PFMA but also others including departmental instructions). For example, a review of health services would also need to consider the laws related to patient privacy, handling and storing on prescription medications etc.

8.3.4 Established rules and procedures

The *Public Finances (Management) Act 1995 (as amended)*, Financial Instructions and the Finance Management Manual set out the rules and procedures to be followed in the management of public moneys. All internal auditors carrying out public financial audits must have a sound understanding and working knowledge of the Act and the Instructions. They must equally have a sound understanding and working knowledge of the *Public Services (Management) Act 1995*, General Orders, and the Code of Conduct.

The auditors must identify and refer to other authorities as appropriate. For instance, the *Organic Law on Provincial Governments and Local-level Governments*, when auditing Provincial Administrations and District Administrations, or *Hospitals Act* when auditing a public hospital. It is also required to have a good understanding of other Acts that relate to good governance such as the *Organic Law for the Independent Commission against Corruption, Whistleblower Act, Digital Government Act* etc.

8.3.5 Conduct Risk Assessment

There needs to be a collaboration between management, risk officers, or subject matter experts to identify inherent risks (risks before controls) and residual risks (risks after current controls).

When reviewing risk, the assessment also needs to consider both impact (financial, reputational, operational) and likelihood.

8.3.6 Prioritise Risks & Develop the Audit Plan

As with any risk framework, risks are categorised (eg, “High,” “Medium,” “Low”) and you would allocate audit resources to “High” risks—these become top priorities in the audit work program. Lower-risk areas may receive periodic or rotational reviews.

8.3.7 Execute Risk-Based Audits

Scope each audit according to the identified risk. For instance, if within procurement, the management of contracts, is high-risk, the audit might delve deeply into tender processes, contract performance management, and contract controls. The aim is to test controls specifically designed to mitigate the identified high risks, rather than generic compliance checklists.

8.3.8 Report & Follow-Up

Emphasise significant, high-risk findings in reports and work with management and the Audit Committee to track remediation efforts, ensuring the biggest risks are addressed quickly.

8.3.9 Practical Considerations for Agencies

Internal audit, particularly a highly functioning audit committee, is a mandatory requirement but often difficult to implement, particularly in PNG

where there are insufficient resources assigned or audit skills are difficult to recruit. To support this please consider:

- The internal audit's risk assessment should be tied directly to the agency's strategic mission (e.g., delivering essential services, controlling public expenditures). Focussing on what matters.
- Smaller agencies with fewer auditors must be especially selective—risk-based planning is key to making the most of limited audit capacity. Also consider collaborating with other agencies to share resources to deliver high-risked audit plans.
- Political, economic, and environmental factors can shift rapidly in PNG and an audit committee is essentially for establishing the minimum expectations for risk assessment. Internal auditors or those officers assigned to audit functions, should establish a routine (e.g., quarterly) to update the risk assessment.
- Departmental heads and management is ultimately responsible for addressing high risks. A risk-based audit approach fosters closer collaboration, as both internal audit and management share a common focus on the biggest threats to success.
- Keep clear records of how risks were identified, how they were rated, and why certain areas were selected (or not selected) for audit. This transparency boosts credibility with the Audit Committee and external auditors.

A major challenge in PNG is implementing audit findings – this requires ongoing efforts to ensure the 'tone at the top', it's not just the oversight of audit committees but the consistent and ongoing efforts to not tolerate lack of priority placed on implementing audit findings for high-risk areas.

8.3.10 How Internal Audit & The Audit Committee Collaborate

Risk-based auditing is the cornerstone of modern internal audit. By aligning the audit program with the areas that pose the greatest threat to an agency's

financial integrity and mission, internal audit provides maximum value. This approach not only meets the PFMA's call for responsible financial management but also ensures efficiency—limited auditing resources target the issues that matter most.

The draft risk-based audit plan should be presented to the Audit Committee for discussion and endorsement (aligns with INTOSAI GOV 9140). If a high-risk situation emerges mid-year (e.g., a new IT system or a budget shortfall), internal audit may revise the plan in consultation with the Audit Committee.

Summaries of major risks, audit findings, and recommended actions are shared regularly with the committee to ensure timely decisions.

8.3.11 Quick Checklist

1. Does your internal audit plan clearly link each chosen audit to the agency's top risks?
2. Have you considered emerging or external risks (e.g., climate change, or technology changes)?
3. Do you review and update the risk assessment at least annually (or more frequently if needed)?
4. Is the Audit Committee involved in endorsing risk priorities and discussing high-risk issues?

Further Information	iacd@finance.gov.pg
Version	1.0
Date Issued	30 June 2025