# Understanding the Internal Audit Universe and the annual risk-based internal audit planning process & Risk Management reporting

Presentation by:

Sospeter Thiga
Group Head of Risk & Compliance, CPF Financial Services Ltd

Friday, 24th September 2021

Uphold public interest

# Introduction

**CPA Sospeter Thiga**

- CPA K, CISA, CRA, CERM
- MBA Strategic Management, BA Economics & Sociology – UON
- Group Head of Risk, Compliance and Performance Monitoring – CPF Financial Services Limited.
- 16 years experience in Finance, Assurance & Risk.
- Family man, one wife and 4 children.

# Introduction

LAPTRUST
— Fulfilling Lives —

CPF
COUNTY PENSION FUND

CPF
Individual Pension Plan

CPF
Fulfilling Lives

FINANCIAL SERVICES

**Our Services**

- **Fund Administration**
- **Gratuity Management**
- **Archival Services**
- **Trust fund Services**
- **Training and Consultancy**

LIB Laser Insurance Brokers
A subsidiary of CPF Group

**Insurance Services**

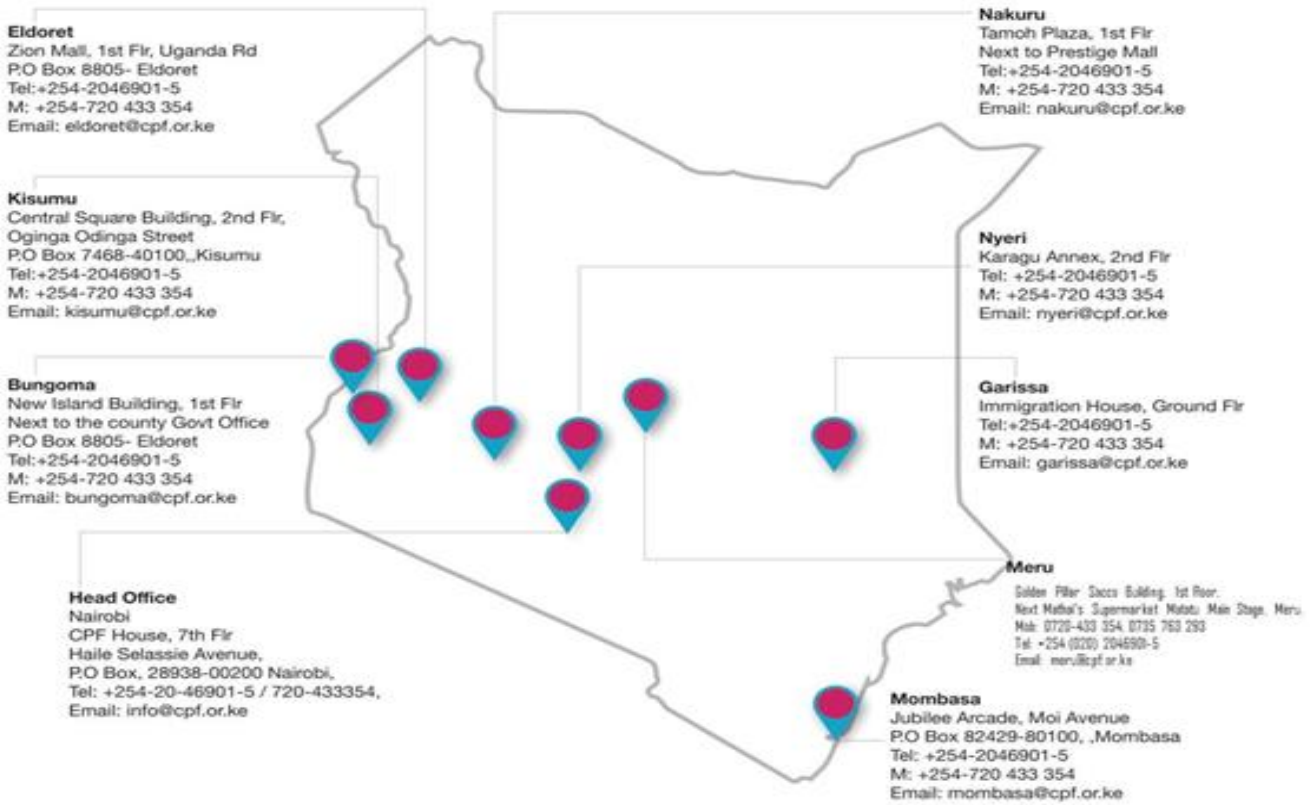
LASER PROPERTY SERVICES
A subsidiary of CPF Group

**Property Services**

LITES
INFRASTRUCTURE • ICT SOLUTIONS
A subsidiary of CPF Group

**Technology, Infrastructure & Renewable Energy**

# Introduction



# Background

- Over the last few years, the need to manage risks has become recognized as an essential part of *good* corporate governance practice.
- This has put organizations under increasing pressure to identify all the business risks they face and to explain how they manage them.
- In fact, the activities involved in managing risks have been recognized as playing a central and essential role in maintaining a sound system of internal control.
- While the responsibility for identifying and managing risks belongs to management, one of the key roles of internal audit is to provide assurance that those risks have been properly managed.

# The Audit Universe

- An audit universe represents a range of potential audit activities to be carried out by internal audit function.
- It consists of several auditable entities, processes, systems and activities.
- As such, the audit universe is determined and updated based on critically of the risk areas that could be subject to audit.
- The audit universe includes projects and initiatives related to the organization's strategic plan, and it may be organized by business units, product or service lines, processes, programs, systems, or controls.

# Risk Based Internal Audit

- IIA defines risk based internal auditing (RBIA) as a methodology that links internal auditing to an organization's overall risk management framework.
- RBIA allows internal audit to provide assurance to the board that risk management processes are managing risks effectively, in relation to the risk appetite.

# Risk Based Internal Audit

**IPPF Standard 2010 – Planning**

- The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

Interpretation:

- To develop the risk-based plan, the chief audit executive consults with senior management and the board and obtains an understanding of the organization's strategies, key business objectives, associated risks, and risk management processes.
- The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.

# Risk Based Internal Audit

**IPPF Standard 2120 – Risk Management**

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

**Interpretation:**

Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- *Organizational objectives support and align with the organization's mission.*
- *Significant risks are identified and assessed.*
- *Appropriate risk responses are selected that align risks with the organization's risk appetite.*

# Risk Based Internal Audit

- *Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.*

  - The internal audit activity may gather the information to support this assessment during multiple engagements.
  - The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.
  - Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

# Feedback Time

Have you formally implemented RBIA at your organization?

https://PollEv.com/multiple_choice_polls/I558eLy2cz3IiYXu2LLly/respond

# Feedback Time

As a member of the Audit Committee, are you aware of the RBIA approach in your institution?

https://PollEv.com/multiple_choice_polls/BUA3kyCN5iWDYSfwATxVS/respond

# Risk Based Internal Audit

- RBIA seeks at every stage to reinforce the responsibilities of management and the board for managing risk.
- If the risk management framework is not very strong or does not exist, the organization is not ready for RBIA.
- More importantly, it means that the organization's system of internal control is poor.
- Internal auditors in such an organization should promote good risk management practice to improve the system of internal control.
- Where RBIA is new to an organization, the head of internal audit will need to market the concept to management and win their support, particularly since it may mean a change for them in the way that they think about risk.

# Drawbacks of RBIA

- RBIA is at the cutting edge of internal audit practice. As a result, it is an area that is evolving rapidly and where there is still little consensus about the best way to implement it.
- It is more difficult to manage than traditional methodologies.
- Monitoring progress against an annual plan that is constantly changing is a challenge.
- Setting targets and appraising staff may become more complex.

# Advantages of RBIA Approach

By following RBIA internal audit should be able to conclude that:

1. Management has identified, assessed and responded to risks above and below the risk appetite.
2. The responses to risks are effective but not excessive in managing inherent risks within the risk appetite.
3. Where residual risks are not in line with the risk appetite, action is being taken to remedy that.
4. Risk management processes, including the effectiveness of responses and the completion of actions, are being monitored by management to ensure they continue to operate effectively.
5. Risks, responses and actions are being properly classified and reported.

# Advantages of RBIA Approach

This enables internal audit to provide the board with assurance that it needs on three areas:

1. Risk management processes, both their design and how well they are working
2. Management of those risks classified as 'key', including the effectiveness of the controls and other responses to them
3. Complete, accurate and appropriate reporting and classification of risks

# Implementing RBIA

The implementation and ongoing operation of RBIA has three stages.

- Stage 1: Assessing risk maturity

Obtaining an overview of the extent to which the board and management determine, assess, manage and monitor risks. This provides an indication of the reliability of the risk register for audit planning purposes.

- Stage 2: Periodic audit planning

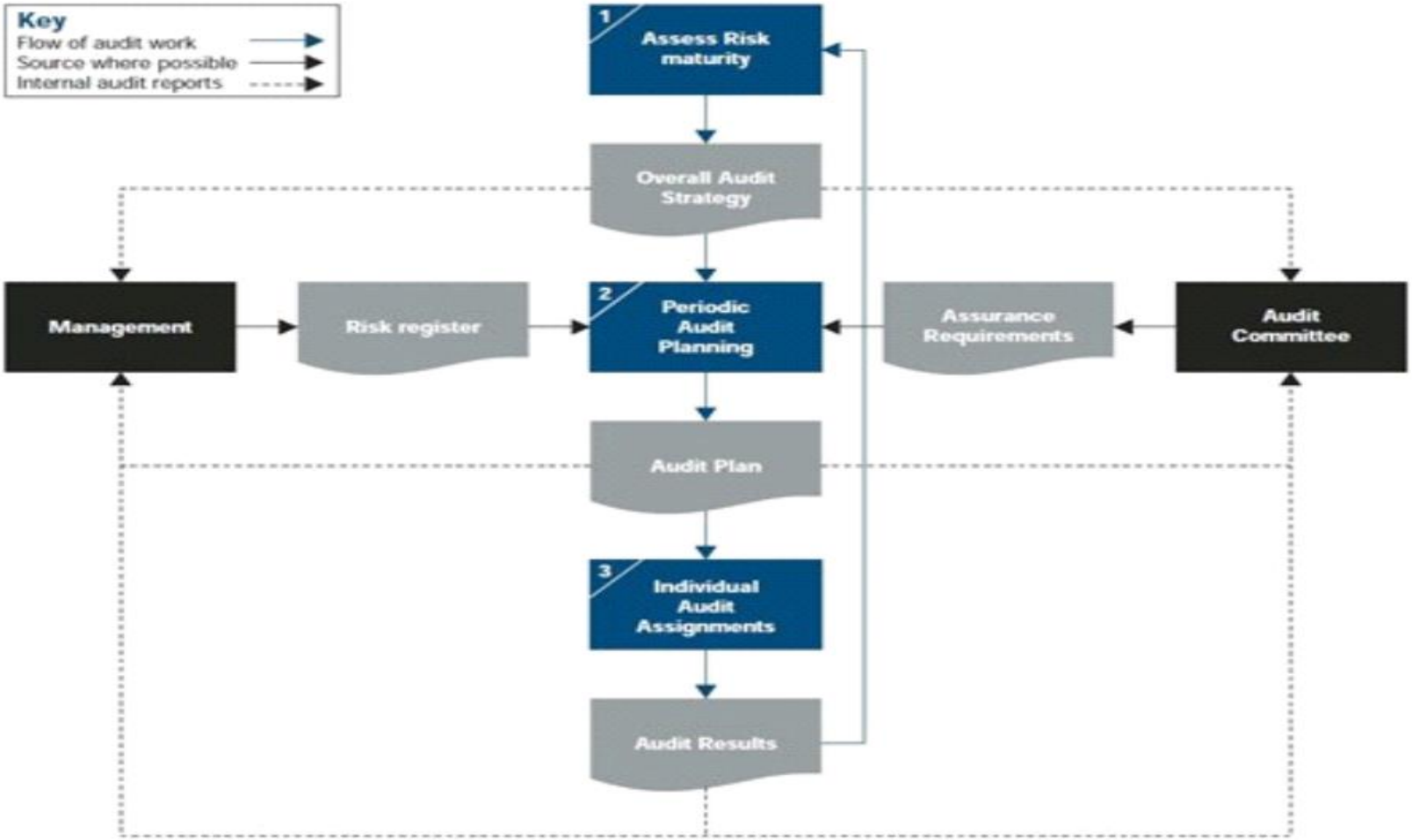
Identifying the assurance and consulting assignments for a specific period, usually annual, by identifying and prioritizing all those areas on which the board requires objective assurance, including the risk management processes, the management of key risks, and the recording and reporting of risks.

# Implementing RBIA

- Stage 3: Individual audit assignments

Carrying out individual risk-based assignments to provide assurance on part of the risk management framework, including on the mitigation of individual or groups of risks.

# Implementing RBIA



# Stage 1: Assessing Risk Maturity

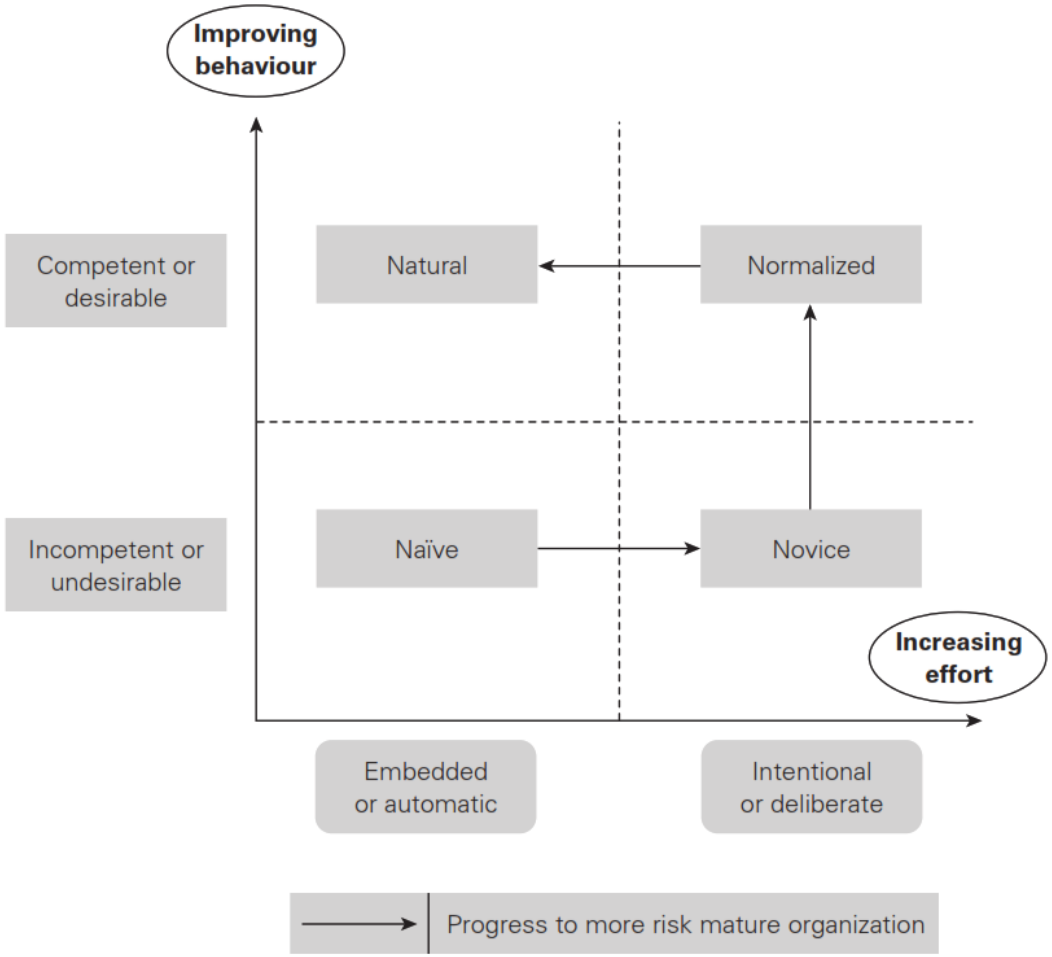
The first stage of RBIA is to review the level of risk maturity. There are three objectives to this stage, which are to:

1. Assess the risk maturity of the organization
2. Report to management and to the audit committee on that assessment
3. Agree an audit strategy

**Actions to achieve the objectives**

1. Discuss the understanding of risk maturity with the board and senior managers.
2. Obtain documents, where they are available.
3. Conclude on the risk maturity (risk enabled, risk managed, risk defined, risk aware and risk naïve).
4. Report your conclusion on risk maturity to management and to the audit committee.

# Risk Maturity Matrix




Hopkin, 2018

# Risk Maturity Matrix

| Level | Status (4Ns) | Characteristics (FOIL) |
|---|---|---|
| 1 | **Naïve**<br>Level 1 organizations are unaware of the need for enterprise risk management and/or do not understand the benefits that will arise. | **Fragmented**<br>Risk management activities are fragmented and focused on legal compliance activities, such as health and safety. |
| 2 | **Novice**<br>Level 2 organizations are aware of the benefits of enterprise risk management, but have only just started to implement an ERM initiative. | **Organized**<br>Actions are planned to co-ordinate risk management activities across all types of risk, although plans may not have been fully implemented. |
| 3 | **Normalized**<br>Level 3 organizations have embedded ERM into business processes, but management effort is still required to maintain adequate ERM activities. | **Influential**<br>Embedded ERM processes are influencing processes and management behaviours, but this may not yet happen consistently or reliably. |
| 4 | **Natural**<br>Level 4 organizations have a risk-aware culture with a proactive approach to ERM and risk is reliably considered at all stages to gain competitive advantage. | **Leading**<br>Consideration of risk is a substantial factor in making business decisions and decisions about strategy are led by ERM considerations. |

Hopkin, 2018

# Stage 1: Assessing Risk Maturity

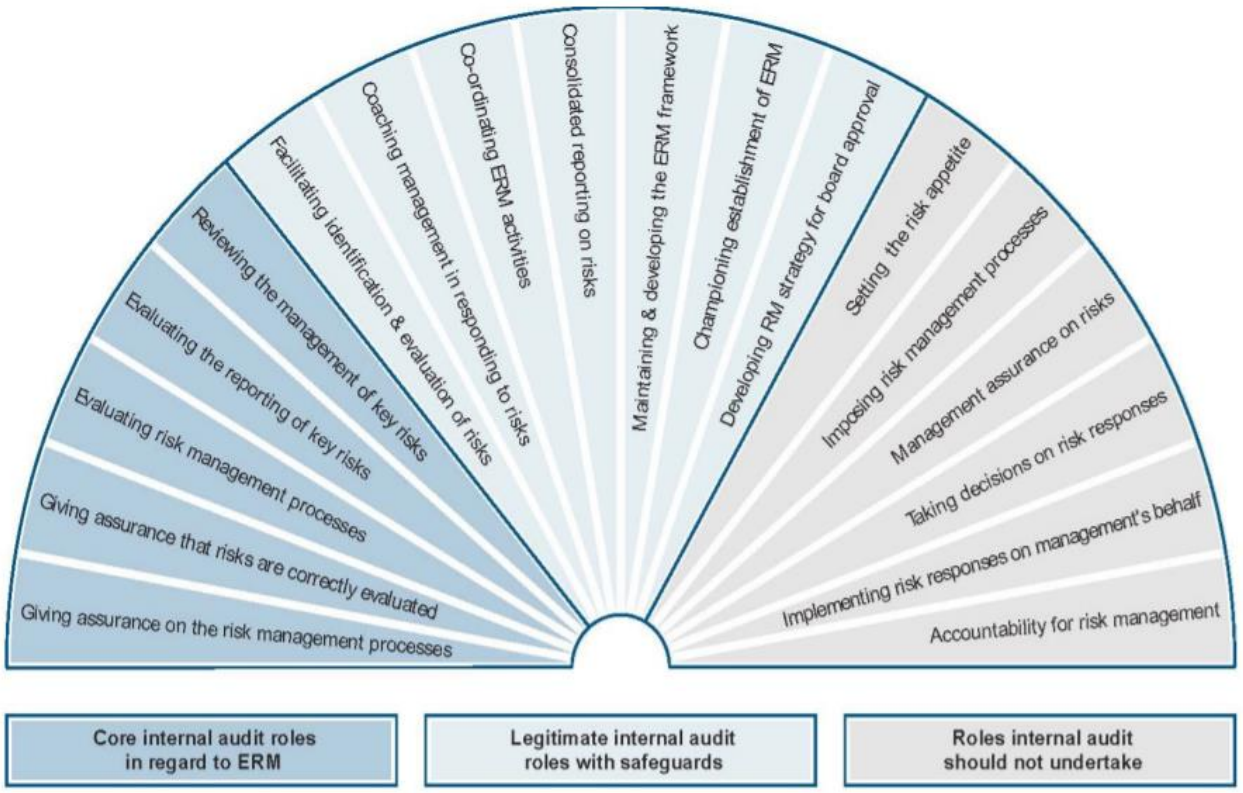
5. Work with management to identify any actions they propose to take as a result of this assessment
6. Decide on the audit strategy
    a) The type of assurances that you expect to be able to give.
    b) The framework that will be used for your audit planning.
    c) The type of consulting services that you expect to provide.

***Mixed risk maturities**

It is possible that one part of an organization may be risk managed and another risk aware. Alternatively, an organization may be risk managed when it comes to one type of risk, for example, market risk in a bank, but risk aware for another type of risk.

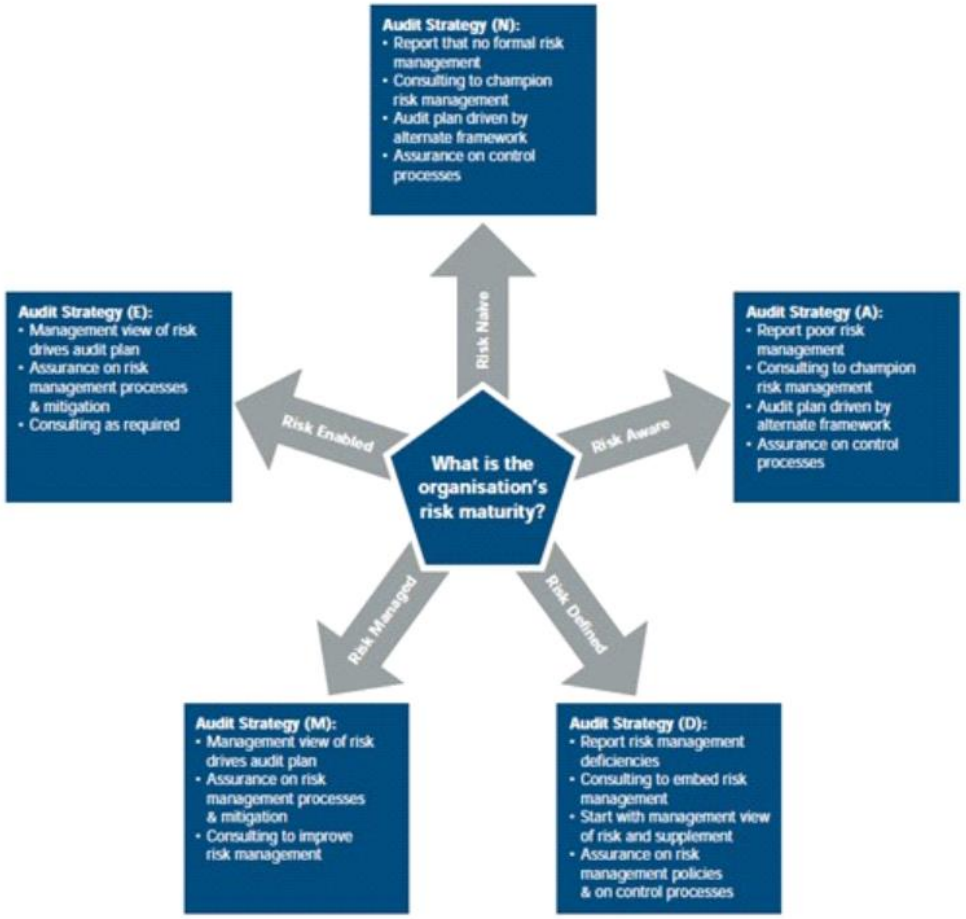
In this case, internal audit should not conclude that the whole organization is risk managed. It should report the dangers of having a patchwork of risk maturities and devise audit strategies separately for the different parts of the organization.

# Stage 1: Assessing Risk Maturity




The role of IA in ERM

# Stage 1: Assessing Risk Maturity



# Stage 2: Periodic audit planning

RBIA is not about auditing risks but about auditing the management of risk. Its focus is on the processes applied by the management team.

The objectives of this stage are to:

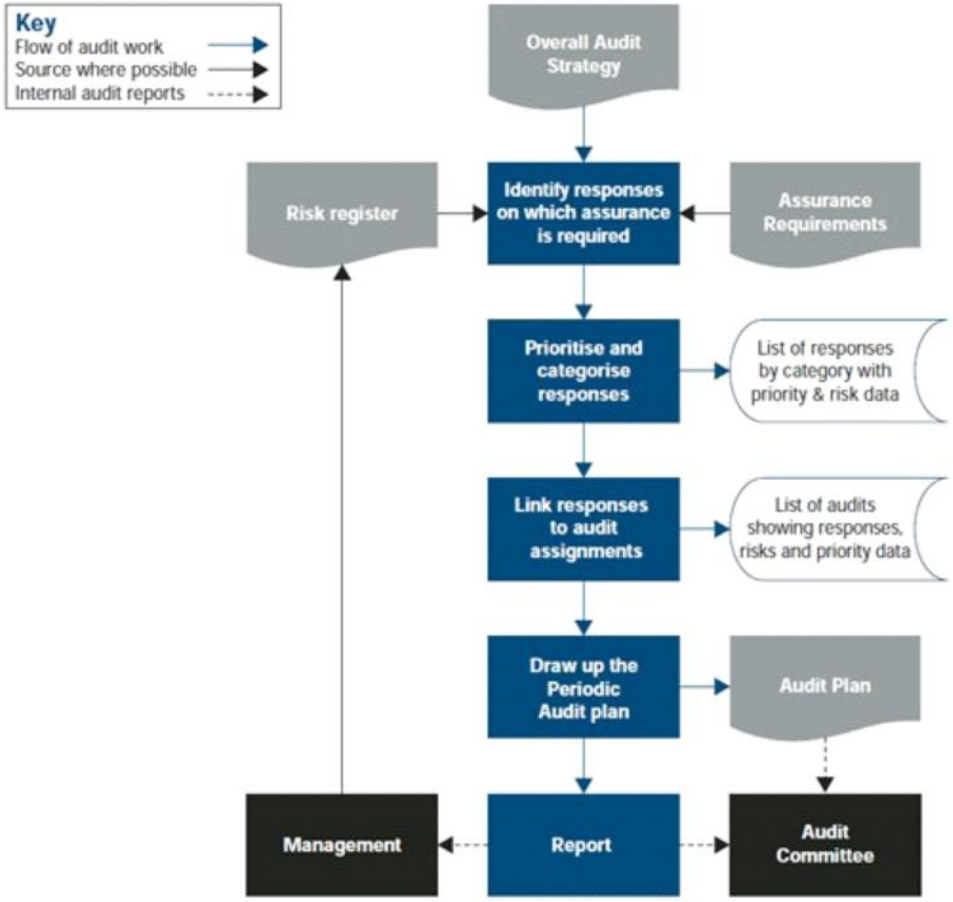
1. Agree all the risk management responses and risk management processes on which objective assurance from internal audit is required
2. Produce an audit plan which lists all audits to be carried out over a specified period - usually a year.

# Stage 2: Periodic audit planning

**Actions to achieve the objectives**

1. Identify the responses and risk management processes on which objective assurance is required.
2. Categorize and prioritize the risks
3. Link risks to audit assignments
4. Draw up the periodic audit plan
5. Reporting to management and the audit committee

# Stage 2: Periodic audit planning



# Stage 3: Individual audit assignments

Internal auditors need to spend time with managers, discussing and observing the monitoring controls they apply, rather than re-performing controls or other responses, or analyzing data for themselves.

The objectives of this stage are to provide assurance that, in relation to the business, activity, or system under review and for the processes identified in the audit plan:

1. Management has identified, assessed and responded to risks above and below the risk appetite.
2. The responses to risks are effective but not excessive in managing inherent risks within the risk appetite.
3. Where residual risks are not in line with the risk appetite, action is being taken to remedy that.

# Stage 3: Individual audit assignments

4. Risk management processes, including the effectiveness of responses and the completion of actions, are being monitored by management to ensure they continue to operate effectively.
5. Risks, responses and actions are being properly classified and reported.

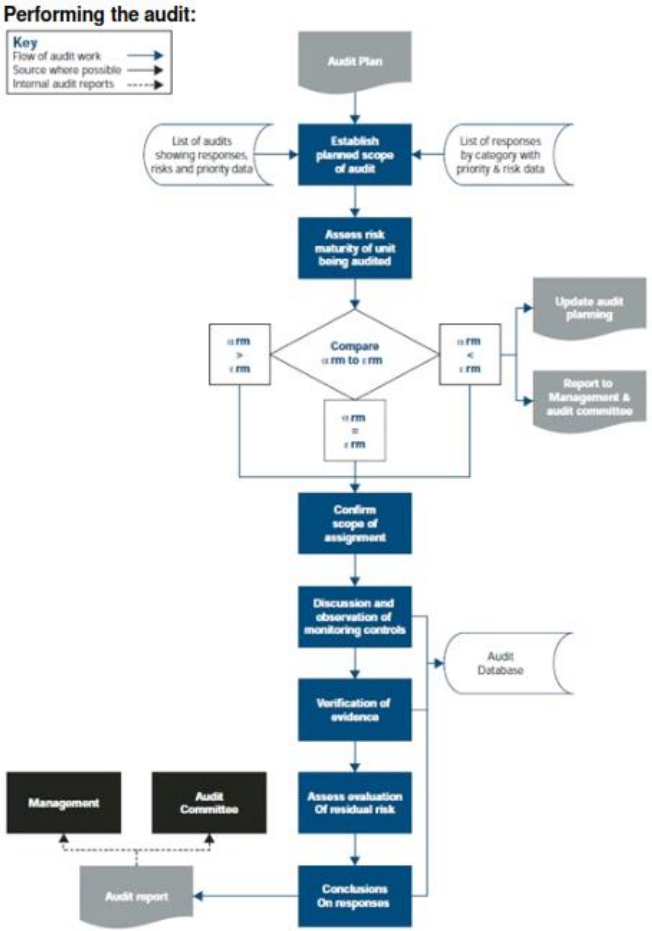
**Action to achieve these objectives**

1. Establishing the planned scope of the assignment
2. Assessing the risk maturity of the unit being audited.
3. Assignment-level conclusions on risk maturity
4. Confirming the scope of the assignment
5. Discussion and observation of monitoring controls
6. Verification of evidence, walkthroughs, re-performance, etc

# Stage 3: Individual audit assignments

7. Documenting the results of the audit work
8. Assessing management's evaluation of residual risks
9. Conclusions on responses and risk management processes covered by the
10. Assignment
11. Reporting and feedback
12. Summarizing the audit conclusions for the audit committee

# Stage 3: Individual audit assignments



# Repeating the cycle of RBIA

- The RBIA methodology is cyclical.
- The interval between revisions in internal audit's assessment of the risk maturity and its audit planning depends on the nature of the organization: how often its circumstances change and how frequently it must report on risk management matters.
- The interval should be agreed with the audit committee.
- Changes to the assessment of risk maturity may change the audit strategy.
- Changes to the risk register, arising from changes to the assessment of risks or from changes in the responses to risks, may change which responses require auditing, the way they are allocated to audit assignments and the priority of the different audits.

# Benefits of RBIA

1. Direct contribution to the organization's objectives
2. Enhances relationship with management
3. Reinforces management responsibility for risk management
4. Enables the achievement of targets
5. Fosters adequate Audit resources mobilization
6. Builds staff expertise
7. Keeps an audit trail for audits

# Benefits of RBIA

**1. Direct contribution to the organization's objectives**

i. An effective risk management framework will improve an organization's governance and its chances of achieving its objectives over the long term.
ii. The RBIA methodology makes a clear and valuable contribution to the risk management framework by providing objective assurance and by facilitating management's efforts to improve the framework.
iii. It ensures that internal audit resources are directed towards assessing the management of the most significant risks

# Benefits of RBIA

**2. Enhances relationship with management**

i. The RBIA approach requires increased management involvement. Since the processes to be covered in audits exist in all parts of the organization, audits may involve managers in departments not visited before.
ii. In order to discuss the responses deployed to manage risks and how management knows these are working properly the internal auditor may need to involve a greater number of more senior managers than might be involved in traditional audits.
iii. RBIA emphasizes management's responsibility for managing risks. This must be stressed during all meetings with managers.

# Benefits of RBIA

**3. Reinforces management responsibility for risk management**

i. RBIA can be implemented fully only in risk enabled and risk managed organizations. One characteristic of this level of risk maturity is that managers have to take responsibility for managing risks. In taking responsibility for risks, managers understand that controls, like other responses to risks, are not the responsibility of internal audit, imposed by internal audit, but are their own responsibility.

ii. Implementing RBIA means that the internal audit activity behaves in a way that reinforces this management responsibility and thus contributes to a stronger risk management culture.

# Benefits of RBIA

**4. Enables the achievement of targets**

RBIA is an effective way to achieve targets set for the internal audit activity, such as:

i. The compilation of an audit plan which ensures the internal audit activity fulfils its charter
ii. Gaining acceptance from management that it takes appropriate action to manage risks within the risk appetite;
iii. Provision of objective assurance in the three areas of risk management normally required; and
iv. Keeping within the budget set for the activity.

# Benefits of RBIA

**5. Fosters adequate Audit resources mobilization**

i. RBIA justifies the number of auditors required. The audit plan, including the resources required, is driven by the proportion of processes and risks on which the audit committee requires objective assurance.
ii. This differs from alternative approaches, where the resources available determine the audits which can be carried out.

# Benefits of RBIA

**6. Builds staff expertise**

i. Internal auditors engaged in RBIA require more people and business skills, such as interviewing, influencing, facilitating and problem solving.
ii. The expansion of the audit universe to cover all risks threatening the organization's objectives requires the internal auditor to conclude on the design and operation of responses to risks in areas that may be new.
iii. This may require specialist knowledge that may be acquired as follows:
    a. Use specialist skills already available within the internal audit activity, e.g., computer auditors.

# Benefits of RBIA

**6. Builds staff expertise**

b. Provide specialist training to auditors with general expertise, e.g., provide training on the regulations and practices related to stress management to an auditor who already a holds an Advanced Diploma in Internal Auditing and Management.

c. Recruit temporary or permanent specialists from inside the organization, e.g., a warehouse manager from one overseas subsidiary could audit warehouse processes in another.

d. Use specialists from outside the organization, e.g., treasury specialists

# Benefits of RBIA

**7. Keeps an audit trail for audits**

i. RBIA ties all aspects of internal auditing together: objectives, risks, processes for responses and monitoring controls, tests and reports.
ii. The relevance of any test can be seen in relation to the opinion on the entire risk management framework because of the relationships set up in the risk and audit universe.
iii. RBIA provides an audit trail from an individual audit report back through tests, processes and risks to objectives, and forward to the audit committee report on whether those objectives are threatened.

# Q & A