Chartered Institute of Internal Auditors

01 February 2023

Risk based internal auditing

Chartered Institute of Internal Auditors

Background

Over the last few years, the need to manage risks has become recognised as an essential part of good corporate governance practice. This has put organisations 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 recognised 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.

We believe that a professional internal audit activity can best achieve its mission as a cornerstone of governance by positioning its work in the context of the organisation's own risk management framework.

What is risk based auditing?

Our definition

IIA defines risk based internal auditing (RBIA) as a methodology that links internal auditing to an organisation'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.

Is the organisation ready?

Every organisation is different, with a different attitude to risk, different structure, different processes and different language. Experienced internal auditors need to adapt these ideas to the structures, processes and language of their organisation in order to implement RBIA.

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 organisation is not ready for RBIA. More importantly, it means that the organisation's system of internal control is poor. Internal auditors in such an organisation should promote good risk management practice to improve the system of internal control.

Where RBIA is new to an organisation, 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.

A dynamic process

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.

But the advantages of RBIA are much greater.

Advantages

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.

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

Read more about the benefits and drawbacks of RBIA

Implementation of RBIA

The implementation and ongoing operation of RBIA has three stages and we have produced detailed guidance on each of them:

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.

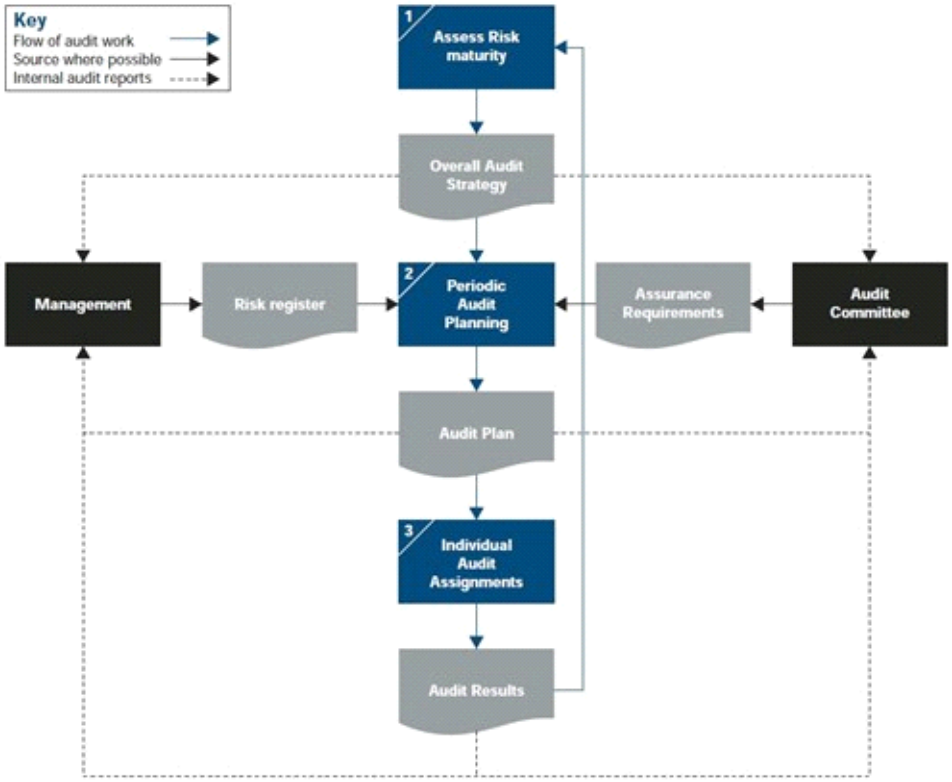
Stage 2: Periodic audit planning

Identifying the assurance and consulting assignments for a specific period, usually annual, by identifying and prioritising 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.

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.

Overview of the stages



Expand this diagram

Next: Risk maturity assessment