Risk based internal auditing

Three views on implementation

David Griffiths
PhD FCA

www.internalaudit.biz

Version 2.2

Contents

Contents

Introduction

Welcome to risk based internal auditing (RBIA). I've been in and around internal audit for 30 years and the aim of this introduction and the associated audit manuals is to pass on some of my ideas and experience.

This book is part of a series:

1. *Book 1: Risk based internal auditing - an introduction*. This introduces risk-based principles and details the implementation of risk based auditing for a small charity providing famine relief, as an example. It includes example working papers.
2. *Book 2: Compilation of a risk and audit universe*. This book aims to show you how to assemble a Risk and Audit Universe (RAU) for a typical company and extract audit programs from it. The audit program in Book 4 is based on the accounts payable audit from the RAU in Book 2
3. *Book 3: Three views on implementation*. (This book). Looks at the implementation of risk based internal auditing from three points-of-view: the board; Chief Audit Executive (CAE); internal audit staff.
4. *Book 4 Audit Manual*. The manual provides ideas about how to carry out a risk based internal audit of accounts payable. It is based around the actual working papers, similar to those in the audit from Book 1.

I won't claim that my ideas in this book are shockingly original; indeed most are built on accepted thinking and practices. Thanks are due to my colleagues in the Boots Group and contacts gained from the IIA-UK and Ireland (now the Chartered Institute of Internal Auditors) for their help and advice – but the views expressed are my own. My aim in this book is to present some of the principles of internal auditing in a simplified way and make them consistent, based on risk. The reader can then move onto more complex concepts, such as those published by COSO (see the *Links* section of www.internalaudit.biz).

This book looks at the impact of risk based internal auditing when introduced into an organization, based on my experiences. All my books, with their related web site and audit manuals are my view of risk based internal auditing. They are not meant to represent 'best practice' but to be thought provoking. This book is not intended to be a lengthy, well-researched academic treatise, but a simple introduction. I've therefore used an informal, as opposed to an academic, style. I'll leave you to judge whether this works. I would also advise you to look for further information from the links on the website.

Many thanks and happy reading…

David M Griffiths Ph.D. F.C.A.

.

1 Why is risk based internal auditing important?

1.1 Why is understanding risk important?

When Harold Macmillan (UK Prime Minister 1957 - 1963), was asked by a journalist what can most easily steer a government off course, he answered 'Events, dear boy. Events'.

Times don't change; investors and directors don't like unexpected events. Which is why regulators are now requiring organizations to determine the risks which might give rise to these events and, in some cases, disclose them.

But it's not about bureaucracy: an organization that understands its risks, understands its opportunities. However:

- If it doesn't know its risks, it doesn't know the risks it can ***accept***
- If it doesn't know the risks it can accept, it doesn't know the risks to ***take***
- If it doesn't know the risks to take, it doesn't know how to ***grow***
- If it doesn't know how to grow, it will ***wither*** *away*.

If it does not understand its risks, 'Events' will knock the organization back; missed opportunities will hold it back.

So how does any organization control events and seize opportunities? By understanding:

- The risks it faces, both ongoing and in new projects.
- The risks it is prepared to accept.
- The action necessary to manage those risks it is not prepared to accept.

Since the management of the organization is responsible for controlling events and seizing opportunities, they are responsible for specifying objectives and identifying, assessing and managing the risks threatening the achievement of the objectives. The correct operation of these processes is essential if an organization is to achieve its objectives. Stakeholders, including investors and other interested bodies, now expect confirmation that this risk management framework is operating effectively. Just as external auditors provide confirmation concerning the financial accounts, so internal auditors provide this confirmation concerning the risk management framework.

1.2 What is risk based internal auditing?

Risk based internal auditing (RBIA) is the methodology which provides an independent and objective opinion to an organization's management as to whether its risks are being managed to acceptable levels.

RBIA is one of many opinions provided to the board, and audit committee, on corporate governance. These opinions are more conventionally known as 'assurance', which includes the opportunity to indicate why assurance cannot be given, in part or whole.

In implementing RBIA, the assurance required by the board from various functions (for example, health and safety, quality control, insurance, the external auditors) will have to be taken into consideration, and this should be reflected in the internal audit department's charter (terms of reference). It is the internal audit department's responsibility to fulfill the board's requirements; it is the board's responsibility to fulfill the requirements placed on it by legislation and its stakeholders.

The methodology consists of the five core internal audit roles which cover the risk management framework of the whole organization (known as 'Enterprise-wide risk management' (ERM)):

1. Giving assurance that the processes used by management to identify all significant risks are effective.
2. Giving assurance that risks are correctly assessed (scored) by management, in order to prioritize them.
3. Evaluating risk management processes, to ensure the response to any risk is appropriate and conforms to the organization's policies.
4. Evaluating the reporting of key risks, by managers to directors.
5. Reviewing the management of key risks by managers to ensure controls have been put into operation and are being monitored.

The core roles are described in the IIA-UK and Ireland publication, *The Role of Internal Audit in Enterprise-wide Risk Management*. In other words:

Enterprise-wide Risk Management drives Risk Based Internal Auditing

RBIA therefore applies to any risk that threatens the achievement of the organization's objectives. These will include financial, operational and strategic risks, whether internal to the organization, or external.

1.3 What's the aim of this book?

This book provides separate guidance for directors, chief audit executives and internal audit staff on:

- Why risk based internal auditing (RBIA) should be introduced
- How risk based internal auditing can be implemented
- The advantages and disadvantages of RBIA

The aim of this book is to enable an organization to implement RBIA in an effective and efficient manner. It provides details on RBIA which:

- Support current requirements (such as the FRC guidelines for UK quoted companies, COSO internal audit framework for the US and the Institute of Internal Auditors *International Professional Practices Framework (IPPF*)). This book is intended to compliment the IIA-UK and Ireland Guidance *An Approach to implementing Risk Based Internal Auditing.*
- Give support to the use of RBIA as an efficient and effective use of internal audit resources.
- With the other books available from www.internalaudit.biz, provide practical advice to enable implementation, which is:
  - Easily understood by its intended audience.
  - Simple to implement.
  - Useable by any size of internal audit department.
  - Capable of being implemented in stages.

Implementing RBIA - Introduction

The book assumes that readers have an understanding of the regulations regarding risks and internal controls that affect their organization, for example the COSO framework for US organizations, the London Stock Exchange (LSE) Governance Code for UK quoted companies, or the UK Government Internal Audit Standards. While this guidance discusses risk management, it does not consider the subject in great depth.

Every organization is different, with a different attitude to risk, different structure and different processes. This book can only provide advice and ideas for an experienced internal audit department to implement RBIA according to its charter and practical limitations. It is not intended as an internal audit manual to be implemented in every detail, and assumes an appropriate knowledge of internal auditing methods of operation and reporting.

.

2 Guidance for directors

2.1 Why understand risks?

Directors need to understand risks because:

- Your organization has objectives.
- Risks threaten the achievement of these objectives.
- Your organization reacts to these threats by introducing internal controls.
- You therefore need to know that these internal controls are reducing the risks to a level which you approve.

So stakeholders, including investors, trustees, customers, directors, councilors, taxpayers and employees expect an organization to achieve its objectives. Since risks threaten this achievement, regulations around the world are increasingly requiring disclosures on risk.

- United States: *COSO Internal Control - Integrated Framework (May 2013) Principle 7*. 'The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.'
- United Kingdom: *The UK Corporate Governance Code (Sept 2014) Main principle C.2.* 'The board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems.'
- South Africa: *King Code of Governance Principles (June 2012) Principle 4.1*. 'The board should be responsible for the governance of risk'.
- Singapore: *Code of Corporate Governance (May 2012) Principle 11*. The Board is responsible for the governance of risk. The Board should ensure that Management maintains a sound system of risk management and internal controls to safeguard shareholders' interests and the company's assets, and should determine the nature and extent of the significant risks which the Board is willing to take in achieving its strategic objectives.

Assuming your organization has embedded risk management into its processes, how can you ensure that the organization's risks are being properly controlled in order to achieve your objectives?

That's where internal audit comes in. Its responsibility is to agree with the board (or board audit committee) which risks should be checked as being properly controlled. The methodology that internal audit will use is *risk based internal auditing*.

2.2 What is risk based internal auditing as far as I'm concerned?

So risk based internal auditing (RBIA) is the methodology which the Internal Audit Department uses to provide an opinion to the board as to whether risks are being managed to a level considered acceptable by the board.

For example, an important risk management process is a system of internal control that reduces risks to a level that the board considers acceptable, the 'risk appetite' of the organization. The simplified diagram below shows the relationship between the risk appetite (dotted line) risks before they are controlled (inherent risks) and risks after they are controlled (residual risks).

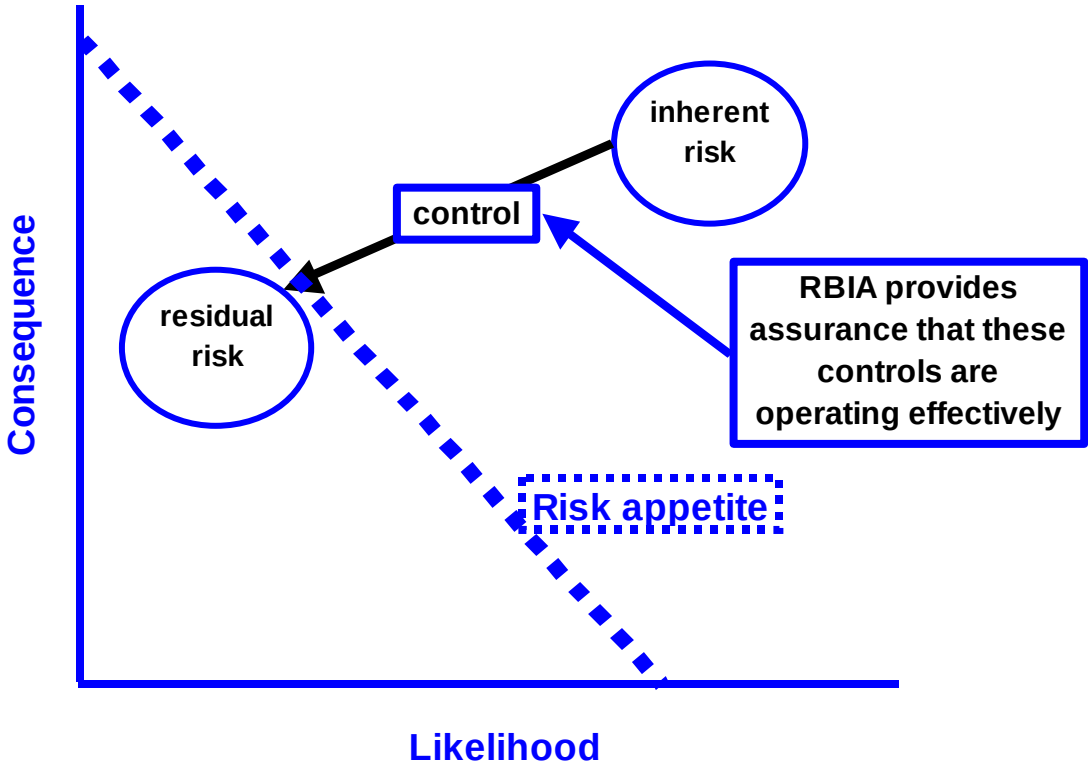


Fig 1 What is Risk Based Internal Auditing?

2.3 What is the responsibility of the directors?

In order for RBIA to be effective, directors need to ensure that the risk management framework includes the following:

- A specification of the objectives.
- That directors and managers have identified and assessed the risks threatening their organization's objectives and have developed a system of internal control, or other suitable response, to reduce this threat to below their risk appetite, or report to the board where this is not possible.
- That inherent risks are recorded and assessed in some way that permits them to be ranked in order of threat.
- That board has approved a risk appetite for the organization on such a basis that risks can be easily identified as being above, or below, the risk appetite.

- That responsibility for providing an opinion on the risk management framework is defined. This will include defining the responsibilities of management, external audit, internal audit and any other functions that provide assurance, such as HR, Finance, Loss Prevention and Health and Safety departments.

In most large organizations a suitable risk management framework should be in place, because they are affected by regulations which require the identification, assessment, management and monitoring of risks. Additional work may be required to ensure all significant risks have been identified and to record all risks and score these in order to prioritize them. None of these tasks is the responsibility of the internal audit department, although it could act as champion, and even project manager, for risk management, especially in the early stages of introduction.

Some boards may wish to define different risk appetites for different parts of their organization (for example corporate HQ and overseas subsidiaries) or different processes (for example new product development and financial transactions).

2.4 What are the pluses and minuses?

- The effectiveness of the internal audit department can be clearly seen. The significant risks are documented in the Objectives, Risks and Controls register ORCR) and the audit plan shows which risks are to be assessed as having adequate controls - and which risks will not be assessed. You are therefore in a position to consider if the audit plan fulfils your requirements in assuring the board that risks are being properly controlled.
- Since RBIA involves providing an opinion to directors on the risk management processes over all risks, the audit plan may contain audits not carried out by auditors before, for example, covering risks affecting public relations, supply chain management and treasury. Internal audit's responsibility is limited to ensuring managers have identified their risks and have responded appropriately to reduce them to below the risk appetite. If specialist knowledge is required to do this, it may be available from within the organization, and suitably qualified staff could be seconded to internal audit, if they are independent of the area being audited. If such specialist knowledge has to be obtained outside, additional costs will be involved. In addition, there may be resistance from managers not used to audits of their areas of responsibility.
- By concentrating on audits of inherent risks above the risk appetite, some audits previously considered important might disappear. These could include audits of small overseas subsidiaries, 'petty cash' and the Staff Social Club.
- RBIA directs scarce internal audit resources at checking the responses to the risks that present a serious threat to an organization and regulations are now requiring directors to ensure these risks are properly managed. RBIA thus provides directors with an opinion that this is happening, or a warning that it isn't.
- However RBIA requires that the organization has a complete, structured, prioritized list of inherent risks. This may list several thousand risks and, since risks are a management responsibility, will involve senior management resources to compile it. However, once compiled, such a list needs only to be kept up-to-date by periodic revisions and is required for other purposes, such as management decision-making.
- One aim of RBIA is to check that the system of control is reducing risks to below the organization's risk appetite. The board should therefore have formally approved the risk appetite in the same terms as used for prioritizing the risks (usually likelihood and consequence). This is a complex issue and boards may be reluctant to define the risk appetite in such exact terms.

- One benefit of RBIA is that, not only should it highlight risks that are not properly controlled; it should highlight risks that are over-controlled and therefore consuming unnecessary resources.

The adoption of risk based internal auditing has direct benefits for all directors, or their equivalents in all types of organizations.

2.5 I've got some questions

It's all very well you saying drop audits of petty cash, but if my local authority auditors don't do these audits and there is even a small fraud, the council's name appears in the local newspaper as wasting taxpayers' money. How do you solve this?

It is unfortunate that a $500 fraud will attract more media attention than the failure of a $2m project to deliver all the expected benefits. Apart from the obvious answer of increasing the number of auditors in order to obtain assurance on the management of low risks, which is not usually an option, the responsibility of managers needs to be considered. Since they are responsible for developing, operating and monitoring the system of internal control, they are accountable for controlling accounting transactions - not internal audit. Thus, the controls which management uses to monitor risks need to be considered. For example, do managers occasionally observe, without warning, the counting of cash floats, do they receive regular confirmation that the petty cash float has been counted by an independent member of staff? While this is additional work for managers, the cash floats are their responsibility, not those of internal audit. In addition, involvement by management emphasizes to staff that controls are considered important.

How do I set a risk appetite?

Deciding on a risk appetite is a complex issue and this book is not intended to provide advice on risk management. However a brief explanation is possible. For more details, the references in 'Further reading' should be checked, for example the 'Orange Book: Management of Risk - Principles and Concepts' available on the UK Government's website is applicable to any organization.

Although there are other business reasons for setting a risk appetite, the management of risk requires a level against which a risk can be compared to determine if it needs a response to reduce it. The system of controls which reduces risks to below this level can be considered as 'operating effectively'.

A risk appetite can be defined by firstly defining the levels of consequence for an organization. For example:

Loss of cash flow if risk occurs	Less than $5,000	$5,001 - $50,000	$50,001 - $1m	$1m - $5m	Over $5m
Description	Immaterial	Small	Significant	Major	Catastrophic
Consequence score	1	2	3	4	5

These levels can also be set for a subsidiary, or other unit in a large organization.

Risk appetite can then be defined as a combination of likelihood and consequence. For example risks with a consequence score equal to, or greater than 3, with a likelihood of 'certain' will not be tolerated, assuming they can be cost effectively controlled. There will probably be a need to set a higher risk appetite for new ventures, in order not to stifle opportunities.

It would be possible to set a risk appetite so high that few, if any, risks exceeded it. However, there will still be a need to comply with any regulations requiring 'effective controls'. The risk appetite should therefore be set at a level below which all risks are considered 'effectively controlled'.

3 Guidance for Chief Audit Executives

3.1 Why should I read this?

Directors are expected to understand the risks their organization is facing; *managers* are expected to identify, assess, monitor and report these risks; the *Chief Audit Executive (CAE)* or *Head of Internal Audit* is expected to provide an opinion that risk management processes are effective. Risk based internal auditing provides the means to do this.

3.2 What's fundamentally different?

If you accept:

- internal auditing is fundamentally about internal controls, and
- Internal controls are necessary to mitigate risks (know of an internal control which doesn't mitigate a risk?)

then *all* internal audit is risk based!

So there is no fundamental difference between, so-called, *risk based internal auditing* and any other sort of internal auditing. Risk based internal auditing is just pushing out internal audit to new boundaries:

- Providing opinions on risks threatening the achievement of all the organization's objectives.
- Considered by the board and audit committee as an essential participant in ensuring the organization's objectives are achieved.
- Regular contact with all senior management.
- Auditors having a wide range of experience.

Book 1 goes into more detail about the new boundaries.

Since management are responsible for specifying objectives and identifying risks, there is one important change for internal audit:

- Risk based internal auditing (RBIA) is driven by the organization's list of objectives and risks, not internal audit's. RBIA is therefore concerned with all the organization's risks, not just those related to finance (and IT) or within internal audit's area of expertise.

The 'traditional' scope of internal audit therefore changes from one where it is in control to one where it is dependent on others.

3.3 Can I carry on as though nothing has happened?

If you work for an organization not subject to regulations requiring it to understand its risks; probably. Although whether you are providing what your board wants is another matter...

If you work for an organization which has to determine and assess its risks; probably not. If an organization determines and assesses its risks, it is likely that it will want an opinion as to whether these risks are being managed to what the board considers an acceptable level. That's where you come in!

3.4 What is RBIA as far as I'm concerned? What are the challenges?

If RBIA is to provide assurance on those risk management processes which cover all significant risks threatening the objectives of the organization, there are four elements which the CAE needs to consider:

1. The extent to which the board and management determine, assess manage and monitor risks. (The 'risk maturity' of the organization).
2. The existence of a risk register (known in these books as an Objectives, Risks and Controls Register), which lists all objectives and significant risks, and the extent to which this may be relied upon for audit planning.
3. The compilation of an audit universe, which lists those audits aiming to provide an opinion whether all inherent risks above the risk appetite are being properly managed.
4. The conduct of individual audits, which conclude on whether inherent risks above the risk appetite are being controlled to reduce them to within the risk appetite.

These elements are described in Book 1 'Risk Based Internal Auditing - An Introduction'.

The challenges in considering these elements are

1. Getting the board and audit committee to understand the new scope of internal audit.
2. Getting senior management (especially those outside finance) to understand the new scope.
3. Forming relationships with any functions responsible for 'risk management'.
4. Getting the risk maturity right (Book 2 gives details).
5. Getting the risk register (ORCR) as a basis for the risk and audit universe (RAU).
6. Deriving an audit plan from the RAU.
7. Defining a risk based audit methodology.
8. Training and motivating staff to deliver risk based audits.

The challenges can be divided into those involving:

- people (1, 2, 3, 4,8)
- processes (4,5, 6, 7)

Getting the risk maturity right (4) involves both people and processes.

3.5 People

3.5.1 Board and audit committee

Board members usually like to consider themselves as 'people of action!' and therefore won't always support, and spend time on, what they might consider the increase of bureaucracy in setting up a risk management framework.

However, they are concerned about 'nasty surprises' and failing to obey the new regulations which are appearing in many countries. They need persuading that by identifying and assessing risks they will reduce the likelihood of

- 'nasty surprises' threatening the achievement of their objectives (and therefore their bonuses).

- failing to obey laws and regulations.

Concentrating on the business benefits of risk management and, by implication, benefits to them, is probably the best way of getting their support, which is essential in getting support from management.

3.5.2 Management

So managers have to accept responsibility for risks and understand that controls are not the responsibility of internal audit, and hence imposed by that department, but are now their own responsibility.

This results in a change in the relationship between internal audit and management. The 'traditional' audit approach is to notify management that an audit will take place, probably have an initial meeting to discuss the audit and any management concerns over controls. The auditors then carry out their tests and, unless any material deficiencies are found, the next contact with management is a discussion of the issues found, with recommendations.

The RBIA approach involves management to a far greater extent, and in this respect can represent a *revolution* for some managers, and some internal audit departments:

- The risks to be covered in audits will exist in all parts of the organization and audits will therefore involve managers in departments never visited before. Many risks will be very significant to the organization and the discussion of their controls will involve more senior managers and directors than might be involved in traditional finance orientated audits. These managers may be skeptical about the competence of internal audit staff to understand the issues involved in their areas and will therefore need reassurance.
- RBIA emphasizes management's responsibility for managing risks. Audits will involve more discussion with managers about their risks and their responses to them. There will be an initial meeting with managers, possibly involving a risk workshop to examine risks in greater depth, and contact throughout the audit to discuss issues.
- The closedown meeting will be less about management's (sometimes passive) acceptance of internal audit's recommendations and more about what management are going to do about risks that are not properly managed. There should be less challenge to an audit's findings, as management will understand the reasoning behind them.
- The aims of management and IA coincide; both want to control risks. Thus confrontations, which can arise from the 'traditional' audit approach based on finding errors, should disappear.

The impact of this greater involvement by management is:

- The Board (or its equivalent) needs to establish policies which ensure management understand, and carry out, their responsibilities for risk management. Risk management needs to be embedded in the organization.
- The CAE will be required to 'sell' the concept and need for risk based internal audit (or internal audit with the boundaries pushed out!). A much higher profile may be necessary in non-financial areas in order to pave the way for audits that managers can understand and, hopefully, support.
- Audit staff will have to use more 'people' and 'business' skills, such as interviewing, influencing and problem solving. While most audit staff will welcome the opportunity to move away from audit programs to more risk and business based audits, some members of staff may find this move difficult. Training will certainly be required and some staff may have to be transferred.

3.5.3 Risk management

The 'risk management' function in organizations can take many roles. It is usually responsible for facilitating management's determination and assessment of risks. It is probably responsible for maintaining the organization's risk register. It may be responsible for identifying controls, scoring residual risks and commenting on those above the risk appetite.

The relationship between internal audit and any risk management function is therefore key to the effectiveness of internal audit. Since internal audit cannot begin work without assuring itself of the risk maturity of the organization and the accuracy of the risk register, it therefore has to audit the Risk Management department.

If one person is in charge of both risk management and internal audit functions, this will result in one of his/her departments auditing the other! A possible conflict of interests.

3.5.4 Audit staff

The expansion of the audit universe to cover all risks threatening the organization's objectives requires that the auditor has sufficient knowledge to conclude on the aims noted in section 1.2.

Core roles 1, 4 and 5 involve risk management processes and are unlikely to require knowledge outside that expected of an internal auditor trained in RBIA. Providing an opinion as to whether risks are correctly evaluated, and responses are appropriate (core roles 2 and 3), will require specialist knowledge. This may be acquired as follows:

- Use specialist skills available in the department. For example, the knowledge of computer auditors where controls over access to a computer system require verification.
- Provide specialist training to auditors with general expertise. For example, provide training on the auditing of value added tax payments to an auditor who is a qualified accountant with a basic knowledge of tax calculations. In this case, the plan for the individual audit, including the risks identified, could be checked by a specialist, possibly from the organization's external auditors.
- Recruit specialists from inside the organization. This might be done on a permanent basis, temporary (a year, for example) or for a specific audit. Such specialists would have to be independent of the area they were auditing. For example, a warehouse manager from one overseas subsidiary could audit warehouse processes in another. Training in the internal audit methodology would have to be provided, and the specialist auditor probably teamed up with an internal auditor.
- Use specialists from outside the organization. For example health and safety experts to audit an organization's health and safety processes. Although such specialists may work alone, they should follow the audit methodology and the scope of the audit should be clearly defined. Their audit documentation should meet the standards of the department, and be reviewed to ensure it meets the quality expected.

There are potentially major changes for internal audit staff, particularly if they are used to using audit programs which detail the work to be done, since there will probably be no audit programs! Many of the processes will never have been audited before, and the work required will have to be defined during the audit. This will require staff that can:

- use initiative and creativity
- learn and understand complex processes
- work from basic principles
- organize their work with little direct supervision

- communicate effectively with all levels of management and staff
- write concise but understandable reports

This could represent a considerable challenge for the management of the internal audit department as not all staff may have these qualities if they have been employed on filling out audit programs. Even if they have these qualities they may be unsure of the benefits of risk based internal auditing and be reluctant to move out of their 'comfort zone'.

Selling RBIA to your staff may be your biggest challenge.

3.6 Processes

These are detailed in Books 1 and 2.

3.7 What's in it for me – the pluses and minuses?

3.7.1 Audit resources

RBIA can justify the number of auditors required. Because the audit plan is driven by the proportion of risks on which the audit committee requires assurance, this determines the resources required. This differs from the alternative approach, whereby the resources available are determined by the budget allowed for the internal audit department, which then determines the audits that can be carried out. It also ensures that resources are directed towards checking the management of the most significant risks.

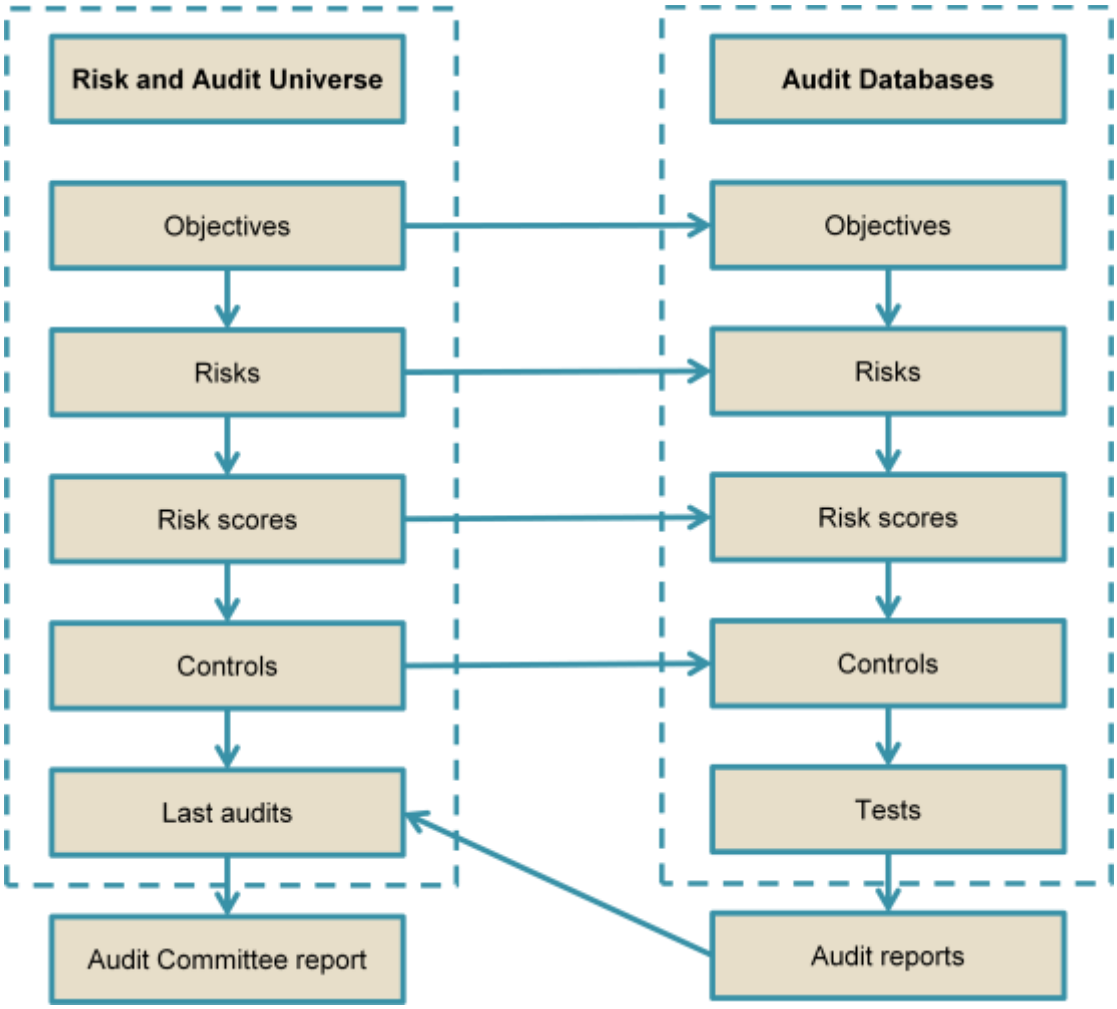
3.7.2 Management of the internal audit department

RBIA has some drawbacks: it is difficult to manage. If the department is used to working to defined audit programs, the time taken to carry out these is known and audits can be planned sequentially. With audits based on risks, many of which will be carried out for the first time and involve contact with senior managers and directors, it is not possible to plan with any degree of accuracy. In practice, staff work on three audits simultaneously, planning for one, carrying out fieldwork for the second and agreeing the report for the third. Setting targets and appraising staff on their achievement can become more difficult. Monitoring progress against the annual plan also becomes more difficult.

The annual plan will change. Audits may be removed, for example if the operation involved is terminated, and additional audits will be included, where new risks are identified. The audit committee should be informed of these changes, as part of the regular reporting.

3.7.3 An audit trail for audits

RBIA ties all aspects of internal auditing together; objectives, processes, risks, controls, tests and reports (see diagram below). 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. This is not always possible where audit programs are used, as it is not always clear why the test is being carried out; the significance if a control is found to be defective; what risk the control is treating and what objective is being threatened by that risk. RBIA provides an 'audit trail' from an individual audit report back through tests, controls and risks to objectives, and forward to the audit committee report on whether those objectives are threatened. In addition the high level objectives, processes, risks, scores and controls form the basis of the individual audit database.



(Figure taken from Book 1)

3.8 I've got some questions

What's the difference between Risk based internal auditing and internal auditing?

The IIA Standards (IPPF) require that audit plans are based on risk (Performance Standard 2010) and that audit engagements take risk into account (2201). So in theory there should be little difference. In reality there may be a considerable difference, especially if the audit department is carrying out compliance audits, or those based on well-defined audit programs. Such audits are usually confined to finance processes and will not cover many of the major risks threatening the objectives of the organization. There is also a danger with audit programs that questions may be missing and staff do not appreciate the underlying risks, and therefore do not necessarily understand the impact of a "no" answer. Audit programs should therefore be limited to those which detail principles and are intended to remind auditors of the basic checks expected.

As we have seen above, risk based internal auditing just pushes out the boundaries of internal auditing.

What's the difference between a risk and the absence of a control?

A risk involves a threat occurring and therefore its description will involve action, while the absence of a control will involve a negative. Therefore, 'Invoices may be paid where no goods or services have been received', is a risk. 'Invoices are not authorized', is the absence of a control.

In addition, a risk will result in the organization losing money, as in the first example above. However, in the second example, if invoices are not authorized, money is not necessarily lost and it is not a risk.

My Internal Audit Department Terms of Reference only covers financial controls. Can I carry out risk based internal audits?

Yes, since you can restrict the risks to only those threatening the financial systems. However, since these may not be the major risks threatening your organization's objectives, it would be advisable to persuade your board to widen the remit of your department.

My department is used to supply staff for covering vacancies and for special projects. Can this continue if I implement RBIA?

There is no reason why not, provided such loss of resources does not prevent you from fulfilling your main obligation to your board or audit committee – assurance that the risk management framework is effective. However, every other activity that the internal audit department does reduces the resources available to provide assurance on risks. Therefore each request should be looked at in that light before committing resources. The CAE should account to the Audit Committee for risks not audited and the work done instead. An IIA-UK and Ireland Professional Issues Bulletin 'Independence and objectivity' provides further details.

4 Guidance for internal audit staff

4.1 Why should I read this?

The adoption of risk based internal auditing effects everyone in the team. The extent of the change will depend on the current methodology used by the department implementing RBIA but it is likely that everyone in the internal audit team will be affected. To understand this section, the previous section, for the CAE, needs to be read as well as books 1 and 2.

4.2 What is RBIA?

Risk Based Internal Auditing is the methodology that provides an opinion as to whether the risk management framework is operating as required by the board**.** RBIA not only involves risks in prioritizing the annual audit plan but also in prioritizing tests within an individual audit, since testing effort can be concentrated on the management of risks with a high control score (inherent risk score minus residual risk score).

4.3 What do I have to do?

4.3.1 Audit approach

The section of this guidance for the chief audit executive considers how the risk maturity of the organization will determine the audit approach. For internal audit staff, there are two approaches:

- **Providing an opinion**: The biggest difference from traditional audit work is that there is much less emphasis on the negative, 'finding faults' and more on the positive, 'confirming controls work'.
- **Consultancy**: This includes facilitating management's identification and assessment of risks and providing advice on the optimum responses to risks. The approach will be used where residual risks are above the risk appetite, and for systems being implemented.

The individual risk based internal audit is very similar to a systems audit in that it involves understanding the processes and controls involved and testing these to ensure they are operating properly. However, it is also very different from a systems audit, particularly those using audit programs, in that it is driven by the risks identified by management. However, this does not mean that management determine the audit work to be done, as the auditor always has the right to carry out whatever work is required to give an opinion whether risks are being managed to an acceptable level (as determined by the risk appetite) or to facilitate and/or agree improvements as necessary.

Example working papers are provided with Book 1 -An introduction, which should give an idea of the work required.

4.4 What's in it for me – the pluses and minuses?

Since RBIA provides assurance on *all* risks, risk based audits can involve areas not usually examined. This is particularly true when previous audit work involved completing audit programs on financial controls, or carrying out compliance audits. The new areas to be audited will be unused to auditors, and there will be much more involvement with managers throughout the audit, not only at the end when presenting findings. Auditors will have to understand more about the practicalities of business and facilitate the implementation of controls accordingly.

RBIA thus presents opportunities, and challenges, for internal audit staff.

4.5 I've got some questions

What skills do I need?

If you are moving away from old-style or traditional audit programs, then you are likely to develop the following skills:

- Marketing yourself, your ideas and your expertise, since you will be working with people who have never had contact with internal auditors. This includes presentation skills.
- Interviewing and listening skills, since you will have to understand the business you are auditing.
- Running meetings and workshops, since these will provide you with your basic building blocks of objectives, risks and controls.
- A wider knowledge of your organization, since you will be auditing high level risks you will need to understand the high level objectives. This includes understanding the external risks threatening your organization.

What techniques should I use?

RBIA doesn't necessarily change the auditing techniques to be used, but *where* they will be used. Physical verification is still vital to ensure what people are telling you should happen is actually happening. Thus you will still continue to use walkthrough tests, sampling of transactions, examination of authorizing signatures and verifying balances. The reason for carrying out these tests is to ensure that the controls that treat risks, and the monitoring controls that ensure these controls are operating, are effective. The tests are not designed specifically to detect incorrect, or fraudulent, transactions. That is management's job.

What about computer assisted audit techniques (CAAT)?

Their use is justified if they are intended to prove controls are effective. If their intention is to detect errors, or fraud, then management should take responsibility for operating them. If internal auditors are used to detect errors then they become part of the control process and not part of the assurance function.

5 Glossary of terms

(Some of these are my definitions! Check out the IIA UK and Ireland – *An approach to implementing Risk Based Internal Auditing* for more official versions)

Assurance: A positive confirmation intended to give confidence that what is reported may be relied upon.

Audit Plan: A list of audits to be carried out in a specified time frame.

Audit universe: A list of all the audits required to provide assurance that all significant risks are properly managed.

Board: A board is an organization's governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a non-profit organization.

Control: Processes which manage risks

Control Score (gap): The difference between the inherent and residual risk scores. The higher the value, the more important the control.

Director: Member of a controlling board, such as a company director, trustee, councilor or governor.

Enterprise-wide Risk Management (ERM): A structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.

Inherent (gross) Risk: the status of risk (measured through consequence and likelihood) without taking into account any risk management processes that the organization may already have in place.

Management of Risks: The implementation of responses to risks, which reduce their threat to below the level of the risk appetite or, where this is not possible, reports the risk to the board (See also *Risk Management Processes*).

Monitoring: Processes which report to management, at appropriate intervals, the success, or otherwise, of the responses to risks.

Residual (net) Risk: the status of risk (measured through consequence and likelihood) after taking into account any risk management processes that the organization may already have in place.

Risk: Circumstances which affect the achievement of objectives

Risk Analysis: the systematic use of available information to determine the likelihood of specified events occurring and the magnitude of their consequences. Measured in terms of consequence and likelihood.

Risk Appetite: The level of risk that is acceptable to the board or management. This may be set in relation to the organization as a whole, for different groups of risks or at an individual risk level. Risks above the risk appetite are considered a threat to the reasonable assurance that an organization will achieve its objectives.

Risk Assessment: the overall process of risk analysis and risk evaluation.

Risk and Audit Universe: The risks register showing the audits which are intended to provide assurance that each risk is properly managed.

Risk Evaluation: the process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.

Implementing RBIA - Glossary of terms

Risk Identification: the process of determining what can happen, why and how.

Risk Based Internal Auditing: the methodology which provides assurance that the risk management framework is operating as required by the board.

Risk Management Framework: The totality of the structures, methodology, procedures and definitions that an organization has chosen to use to implement its risk management processes.

Risk Management Processes: Processes to identify, assess, manage, and control potential events or situations, to provide reasonable assurance regarding the achievement of the organization's objectives.

Risk Maturity: The extent to which a robust risk management approach has been adopted and applied, as planned, by management across the organization to identify, assess, decide on responses to and report on opportunities and threats that affect the achievement of the organization's objectives.

Risk Register: A complete list of risks, identified by management, which threaten the objectives and processes of the organization.

Risk Responses: The means by which an organization elects to manage individual risks. The main categories are to tolerate the risk; to treat it by reducing its impact or likelihood; to transfer it to another organization or to terminate the activity creating it. Internal controls are one way of treating a risk.

Significant Risk: A risk, inherent or residual, above the risk appetite.

6 Version control

Version number	Date issued	Changes made to previous version
1.0.0	30-Jan-2006	Issue of first version
1.0.1	15-Mar-06	Questionnaire removed. Minor changes.
2.0	26-Feb-15	Details of methods removed because it duplicated some content of books 1 and 2
2.1	19-May-2015	Minor amendments to mention the ORCR and the pushing out of internal audit boundaries.
2.2	26-May-2015	Includes publication of revised Book 4