Risk Based Internal Auditing

Three views on implementation

David Griffiths
PhD FCA

www.internalaudit.biz

30 January 2006
Version 1.0.0

Contents

1 Introduction

1.1 Why should I read this?

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 organisations to determine the risks which might give rise to these events and, in some cases, disclose them.
- But it's not about bureaucracy: an organisation 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 organisation back; missed opportunities will hold it back.
- So how does any organisation 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 organisation are responsible for controlling events and seizing opportunities, they are responsible for identifying, assessing and managing risks. The correct operation of these processes is essential if an organisation 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 assurance that risks are being managed to within the organisation's risk appetite***.
- 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 this book, when using the term 'assurance' this includes the possibility that RBIA has found that all risks are not properly managed and therefore assurance cannot be given.

- 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 fulfil the board's requirements; it is the board's responsibility to fulfil the requirements placed on it by legislation.
- The methodology consists of the five core internal audit roles which cover the risk management framework of the whole organisation (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 prioritise them.
3. Evaluating risk management processes, to ensure the response to any risk is appropriate and conforms to the organisation'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 RBIA

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

1.3 What's the aim of this book?

This book provides separate guidance for directors, heads of internal audit 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 organisation to implement RBIA in an effective and efficient manner. It provides details on RBIA which:

- Support current requirements (such as the Turnbull and Smith guidelines for UK quoted companies and the Institute of Internal Auditors *Standards for the Professional Practice of Internal Auditing*). This book is intended to compliment the IIA-UK and Ireland Guidance *An Approach to implementing Risk Based Internal Auditing.* (See *Further Reading* for details of how to obtain this guidance.)
- Give support to the use of RBIA as an efficient and effective use of internal audit resources.
- 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.

- The book assumes that readers have an understanding of the regulations regarding risks and internal controls that affect their organisation, for example, the Turnbull and Smith guidelines to the London Stock Exchange (LSE) Combined 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. Publications listed under 'Further Reading' should be consulted.
- This book differs from my other book, *Risk Based Internal Auditing – An Introduction* in that it is more formal and tries to reflect the generally accepted view of RBIA. I therefore refer to RBIA providing assurance on the management of risk rather than providing an opinion. In particular the book aims to be consistent with:
  - *Risk Based Internal Auditing*, Institute of Internal Auditors (UK and Ireland).
  - *The Role of Internal Audit in Enterprise-wide Risk Management*, Institute of Internal Auditors (UK and Ireland).
  - *An Approach to implementing Risk Based Internal Auditing,* Institute of Internal Auditors (UK and Ireland).
  - *The London Stock Exchange Combined Code*, with the Turnbull and Smith Guidances.

  Details are provided in the 'Further Reading' section. My other book can be downloaded from http://www.internalaudit.biz/.
- Every organisation 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. An *internal audit manual*, using RBIA, can be downloaded from www.internalaudit.biz.
- Please complete the questionnaire at the end of this book so that I can assess how useful it has been and how it can be improved.
- This book is the copyright of D M Griffiths. It may be distributed freely with acknowledgement of the copyright. It may not be sold, in any way.
- Many people have commented on this book during its many versions. Since they may disagree with this final version, I won't embarrass them by including their names. I will say "thank you" to them for their help and encouragement.

2 Guidance for directors

2.1 Why should I read this?

- Risks threaten the achievement of your organisation's objectives. It is therefore in your interest to understand how internal auditing can help you manage these risks.
- Stakeholders, including investors, trustees, customers, directors, councillors, taxpayers and employees expect an organisation to achieve its objectives. Since risks threaten this achievement, regulations are increasingly requiring disclosures on risk.
- The Smith Guidance to the LSE Combined Code clearly defines the role of management in the response to risks (paragraph 4.6):

  The organisation's management is responsible for the identification, assessment, management and monitoring of risk, for developing, operating and monitoring the system of internal control and for providing assurance to the board that it has done so.

- Directors therefore need to ensure that these risk management processes are operating properly and gain assurance that they are effective.

2.2 What is RBIA as far as I'm concerned?

- Risk based internal auditing (RBIA) is the methodology which the Internal Audit Department uses to provide assurance that risks are being managed to within the organisation's risk appetite. In other words: *the processes that manage risks to a level considered acceptable by the board are working effectively and efficiently*.

- 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 organisation. 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).

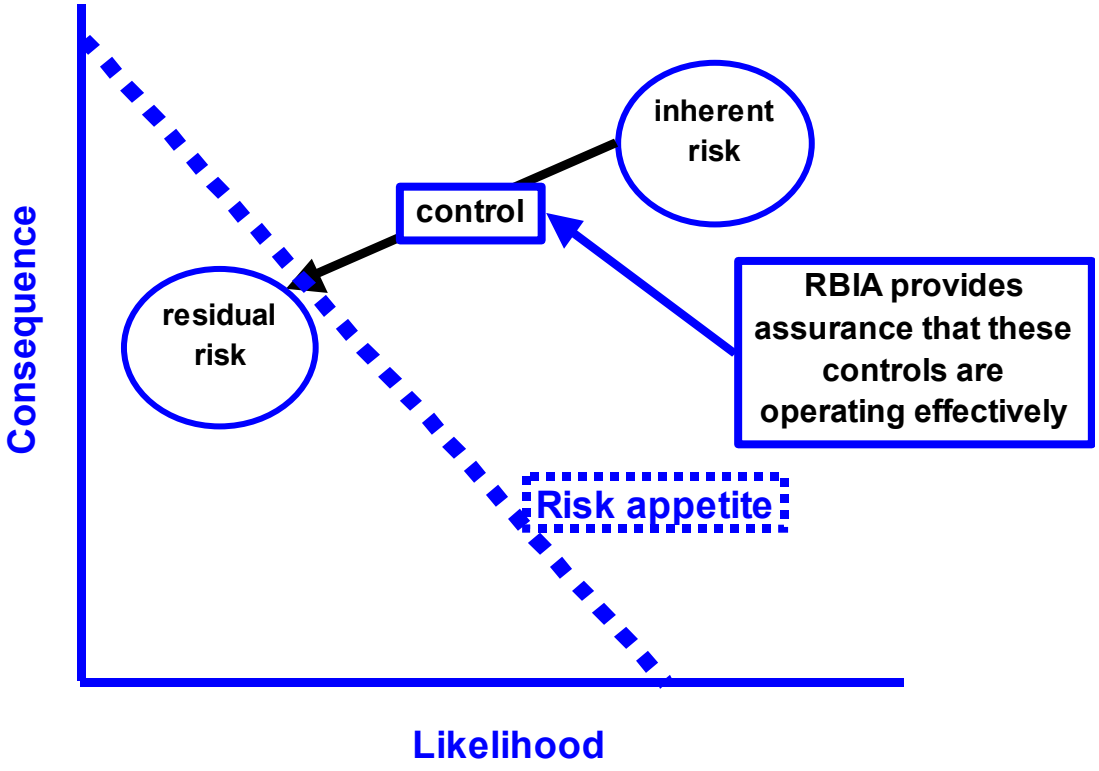


Fig 1 What is Risk Based Internal Auditing?

2.3 What do I have to do?

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

- Directors and managers have identified and assessed the risks threatening their organisation's objectives and have developed a system of internal control, or other suitable response, to reduce this threat to below the risk appetite, or report to the board where this is not possible.
- The inherent risks are recorded and assessed in some way that permits them to be ranked in order of threat.
- The board have approved a risk appetite for the organisation on such a basis that risks can be easily identified as being above, or below, the risk appetite.
- The responsibility for providing assurance 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 organisations a suitable risk management framework will 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 prioritise 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 organisation (for example corporate HQ and overseas subsidiaries) or different processes (for example new product development and financial transactions).
- While it is an ideal that every organisation will have identified its risks at every level, this book aims to be practical and recognises that this will not apply in all cases. So it offers alternative practical solutions, but always on the understanding that risks, and the associated internal controls, are management's responsibility.

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

- RBIA directs scarce internal audit resources at checking the responses to the risks that present a serious threat to an organisation and regulations are now requiring directors to ensure these risks are properly managed. RBIA thus provides directors with assurance that this is happening, or a warning that it isn't.
- However RBIA requires that the organisation has a complete, structured, prioritised list of inherent risks. This may list several hundred 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 organisation's risk appetite. The board should therefore have formally approved the risk appetite in the same terms as used for prioritising 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.
- Since RBIA involves assuring 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 organisation, 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.
- The adoption of risk based internal auditing has direct benefits for all directors, or their equivalents in all types of organisations.

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 use 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 emphasises to staff that controls are considered important.

My company is subject to US regulations. How does Sarbanes-Oxley fit in with risk based internal auditing?

The failure to comply with Sarbanes-Oxley is a risk like any other, which should be included in the risk register and audited accordingly. Sarbanes-Oxley doesn't otherwise have any impact on internal auditing as a concept, The Institute of Internal Auditors is not rewriting any definitions as a result of the legislation. The main impact of Sarbanes-Oxley is to provide additional work for an internal audit department which involves documenting and advising on internal financial controls. There is therefore the danger that it removes internal audit resource from providing assurance on the risk management framework, which is arguably the more important task.

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 H M Treasury website is applicable to any organisation.

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 organisation. 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 organisation.

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 Heads of Internal audit

3.1 Why should I read this?

Directors are expected to understand the risks their organisation is facing; *managers* are expected to identify, assess, monitor and report these risks; the *Head of Internal Audit* is expected to provide assurance that risk management processes are effective. Risk based internal auditing provides the means to do this.

3.2 What is RBIA as far as I'm concerned?

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

1. The extent to which the board and management determine, assess manage and monitor risks. (The 'risk maturity' of the organisation).
2. The existence of a risk register (also known as a 'risk profile'), which lists all 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 assurance that 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 the succeeding sections.

3.3 What's the connection between Internal audit and risk management?

Before detailing how the Head of Audit can implement RBIA, it's important to consider the relationship between the quality of the risk management framework in an organisation (its 'risk maturity') and the approach to be used by the internal auditors. Consideration of this relationship also highlights the difference between 'traditional' internal audit and RBIA.

3.3.1 Responsibility for risk management

- The Smith and Turnbull Guidances clearly state that management is responsible for determining internal and external risks. There is no place for a separate 'Internal Audit' list of risks, or 'off the shelf' lists of risks. Risks should be identified by managers for their organisation. Lists of risks compiled by third parties should not be used other than to check, at the end of the identification exercise, if any risks have been missed.
- If Internal Audit does not consider management has identified all the significant risks, they should discuss the omissions with the management involved. If this does not resolve the issue, it should be reported to more senior management, and the audit committee, as appropriate.
- Internal Audit should never be involved in any risk management activities that might compromise their independence and objectivity. The IIA publication *The Role of Internal Audit in Enterprise-wide Risk Management* has further information.

3.3.2 Response to risks

- Risks may be managed by responding as follows:

  - Tolerate - do nothing. This response is used where it is not possible to cost effectively reduce the risk. Where this applies it is important that the board formally accepts the risk. The need for contingency plans should be considered.
  - Transfer - pass the risk to another party, for example by insurance or contracting it out. Note that outsourcing does not necessarily transfer a risk, it may only change the person responsible for managing it. Insurance does not transfer all the risk; only some or most of the cost of impact.
  - Terminate - remove the circumstances giving rise to the risk.
  - Treat – implement a system of internal control to reduce the risk to below the risk appetite.

- Alternatively an organisation could respond by taking the opportunity – This is an option that applies to tolerate, transfer or treat and particularly applies to new ventures. Risk modelling techniques should be used to ensure that the value at risk is justified by the likely gain.

3.3.3 The changed audit approach

- The 'traditional' audit report usually consists of a confirmation that controls are operating properly (a term not often defined), and makes recommendations where they are not. The making of recommendations by internal auditors, which managers were expected to accept, could result in the assumption that internal audit were responsible for controls and, by implication, risk management.

- However, the Turnbull Guidance (and guidance subsequently issued by other organisations) emphasised the reality: managers are responsible for developing the responses to risks and for deciding the action to be taken if risks are not properly controlled.
- The impact on the internal audit activity is to clarify its role:

  Internal Audit's core role is to provide assurance to the management and board on the effectiveness of risk management.

  Where assurance cannot be given, the onus is on management to implement the appropriate response. Internal audit may still make recommendations, but this is part of a 'consultancy' role.

- Splitting the role of internal audit in this way, has a major implication for the internal audit department:

  Within the context of RBIA, internal audit can only provide assurance where a risk management framework is in place: all other work is consultancy.

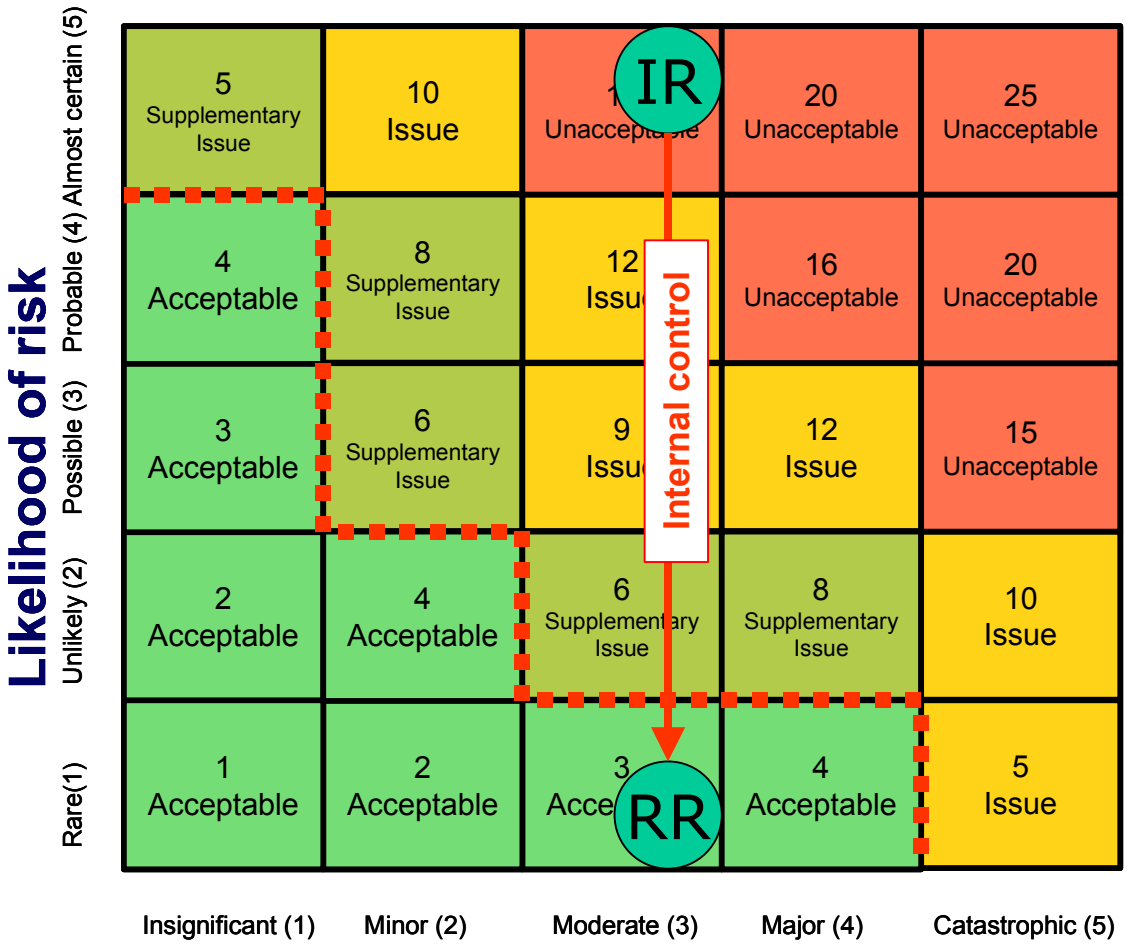
- In practice there has to be compromise, and this book provides practical advice. However, the clarification of the role does show the importance of the organisation's risk maturity to the internal audit approach.

3.3.4 Assessing risks

- The assessment (evaluation/scoring) of risks is outside the scope of this book but the results, and the way they are used, affect the audit approach (assurance or consultancy) which will be discussed in more detail when looking at audit planning.
- The usual method of scoring risks is to assign a level (e.g. high, medium, low), or score (e.g. 1 to 5) to the consequence and likelihood of the risk. Where levels are assigned a numerical value, consequence and likelihood scores may be combined (for example, by multiplication, or by ranking on a grid) to provide an overall score. So for example, the score of the highest risk would be 25 on this basis, when using a 1 to 5 scoring range.

  An example grid is below. The organisation concerned has defined any risk scored at 5, or above, is above its risk appetite, although it considers any risk scoring 9 or above is a key risk and action must be taken to manage the risk (see 3.3.2).

  Appendix A provides further advice on the scoring of risks, using a 1-5 scale.



Unacceptable: Immediate action required to manage the risk

Issue: Action required to manage the risk

Supplementary issue: Action is advisable if resources are available

Acceptable: No action required

Risk appetite, as defined by the board

IR = Inherent Risk RR = Residual Risk

Fig.2 Grid showing the significance of risks

- Both inherent and residual risks are scored. In a numerical scoring system the difference between these scores is known as the *control score*, the assessment of control effectiveness, or the control co-efficient. The higher the control score, the more important the control. Since risks now have a numerical value, they can be sorted to show the greatest inherent risks, greatest residual risks, or those with the greatest control scores.

- In organisations with several operating units, such as overseas subsidiaries, risk consequence may be scored in relation to that unit's value as well as in relation to the organisation as a whole. Thus a risk causing catastrophic failure of a small subsidiary may score a consequence of 5 in the subsidiary's risk register, but only 3 in the corporate risk register.

3.3.5 Management monitoring of controls

- The clarification that management are responsible for developing, operating and monitoring the system of internal control leads to the requirement for management to have processes in place which check that controls are operating properly. Such monitoring controls may include:
  - A monthly checklist of key controls, signed by the staff responsible, as evidence that important checks have been carried out.
  - Management approval of bank reconciliations to check for old, or unusual, items.
  - Management checks of outstanding debtor lists, to ensure credit controls are operating effectively.
- With RBIA, the emphasis on checking controls moves from ensuring key operating controls (such as authorisation of invoices) are effective, to checking that management controls which report failures in key operating controls are effective. While checking that operating controls are effective is still important, there is a danger that management rely on internal audits to confirm their proper operation instead of instigating their own checks.

3.3.6 The RBIA stages

The implementation and ongoing operation of RBIA has three stages (see *An approach to implementing Risk Based Internal Auditing)*:

1. Assess the risk maturity of the organisation
2. Assign the risks to an audit that will examine their management. Set up the Risk and Audit Universe (RAU) and draw up a plan for carrying out audits, usually annual
3. Carry out individual risk based audits and feedback the audit results into the RAU

The diagram below shows the main tasks in these stages:

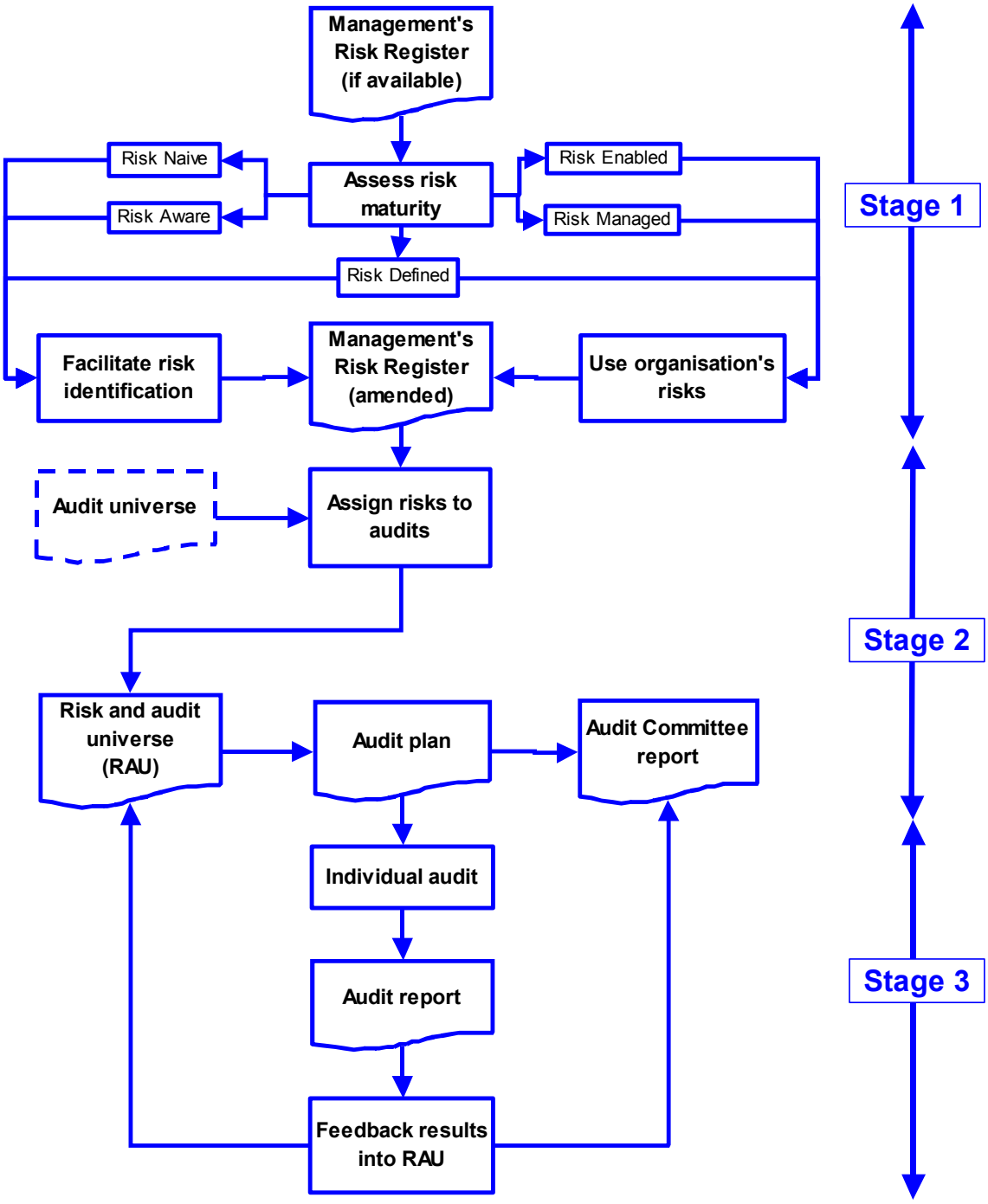


Fig 3 Stages of an audit

3.4 What do I have to do? Stage 1 – assessing the organisation's risk maturity

3.4.1 Introduction

This book is not intended to provide advice on the identification and assessment of risks; it takes an organisation's existing risk maturity as the starting point. Since the risk management framework determines the audit approach, the first stage of RBIA is to determine the level of risk maturity.

3.4.2 Aims of this stage

- An assessment of the risk maturity of the organisation, which will determine how the Internal Audit Department sets up the audit plan and may lead to a report to the audit committee.
- A list of risks (risk register), compiled by managers, which may be incomplete, but with the job title of the person responsible for managing the risk.

3.4.3 Action to achieve the aims

- **Meet the board and senior managers.** Find out what processes have been introduced to improve the risk maturity of the organisation. These processes will include training, risk workshops, questionnaires about risks and interviews with risk managers. The ultimate deliverable from these processes should be a comprehensive risk register and an organisation in which an understanding of risk management is embedded.

  Even if the organisation considers it is only risk aware or risk naïve, there may still be a need to carry out consultancy work to assess the action necessary to raise the risk maturity to risk defined, or higher, as required by the board.

- **Assemble the supporting information available**, such as:
  - The organisation's objectives.
  - The processes for assessing risks, for example by scoring their impact and likelihood, so that they may be prioritised.
  - The board's definition of its risk appetite, in terms of the scoring system used for inherent and residual risks.
  - The procedures to be used by management that will enable them to identify all the key risks threatening the organisation's objectives.
  - A requirement that management consider risks, and their associated controls, as part of decision-making, for example in project approval documents.
  - The risks of the organisation, linked to the objectives they threaten and assessed by their significance. This register (example in appendix B) would ideally show the job title of the person responsible for managing the risk and the controls intended to reduce it to within the risk appetite, or other response considered appropriate. Note that where responses are not considered sufficient to mange controls, this may be noted in the *Potential Issues* column
  - Any other documents, including those on the organisation's intranet, which indicate the commitment to risk management.

- **Audit the risk management processes**. The stages of the risk management maturity of an organisation were defined by the IIA – UK and Ireland in a position statement on RBIA issued in August 2003 (see 'Further Reading'). The assessment of an organisation's risk maturity is based on this position statement. Audit tests to assess the maturity are shown in appendix C, which also includes the key characteristics of each level and the core internal audit role fulfilled by each test.
- **Conclude on the risk maturity**. Issue a report that provides an opinion against each of the core internal roles. An assessment can then be given on the risk maturity of the organisation which can be compared with the Board's own assessment, if one exists. Facilitate, with management, any action they should take to improve the risk management processes of the organisation.
- **Decide on the next action.**

This will depend on the risk maturity of the organisation as follows:

- **Risk enabled:** (Risk management and internal control fully embedded into the operations).

  An understanding of the management of risk and the monitoring of controls will be very sophisticated in this organisation. A complete risk register (example in appendix B) will be available for audit planning. Confidence in the risk management process should enable a range of auditing techniques to be used, from checking the management of individual risks, to those affecting a complete subsidiary.

  It is highly unlikely that internal audit work will find problems relating to its core roles 1, 2 and 3 (see section 1.2) although verification will be necessary. The emphasis of the audit work will be that the risk management processes are working properly, in particular, that key risks are reported to the board and that monitoring of controls by managers is operating. If weaknesses are found, it is unlikely that a recommendation will be necessary, since management will be aware of the action to be taken.

- **Risk Managed:** (Enterprise wide approach to risk management developed and communicated).

  Similar to the risk enabled approach, except more emphasis may be necessary on the core roles 1, 2 and 3 in some parts of the organisation. It may be necessary to facilitate management's proposed action where weaknesses are found.

- **Risk defined: (Strategies and policies in place and communicated. Risk appetite defined).**

  While most managers may have compiled lists of risks, it is possible that these will not be assembled into a complete risk register. Internal audit will act as a consultant to facilitate the compilation of a complete risk register from lists risks already compiled by managers.

  The quality of risk management may vary across this type of organisation. Any individual audit therefore will have to place emphasis on understanding the level of risk maturity in the areas being audited. Where risk management is poor, internal audit will have to facilitate the identification of risks, using workshops and interviews. There will be greater emphasis on core roles 1,2 and 3. It is probable that some consultation work will be necessary to advise managers what action to take where weaknesses are found.

- **Risk Aware: (Scattered silo approach to risk management)**

  No risk register will be available, only a few managers will have determined their risks. Internal audit will act as a consultant to undertake a risk assessment (in conjunction with management) to determine the work required to implement a risk framework which fulfils the requirements of the board. Using the key risks agreed with management, an audit/consultancy plan will be generated which aims to provide assurance that risks are being managed, or advice as to how to respond to them.

  Since this type of organisation does not have a risk management framework, RBIA cannot be implemented. However, individual audits (as detailed in section 3.6) can be driven by risks where management understand risks, or internal audit have sufficient expertise to identify risks. Consultancy work will be necessary to advise on the action to be taken where weaknesses are found.

- **Risk naïve**: (No formal approach developed for risk management).

  As with the risk aware organisation, it will be necessary to promote, or provide consultation on, the establishment of a risk management framework. Until this is done RBIA cannot be implemented.

  Risk driven audits will be possible, but will require management training and risk workshops to determine risks in the areas concerned. Internal audit should not determine risks without management involvement, nor maintain their own list of risks. This will only reinforce management's belief that internal audit are responsible for risk management.

  For organisations that are subject to regulations concerning the adequacy of risk management, the level of risk maturity in risk aware and risk naïve organisations is not acceptable, and the audit committee should be made aware of this. The action above is therefore a short-term solution to producing a limited audit plan.

3.5 What do I have to do? Stage 2 – production of an audit plan

3.5.1 Introduction

- Having assessed the risk maturity of the organisation in stage 1, the auditor can decide what reliance to place on the list of risks provided by management when determining the audit plan. Where the auditor cannot rely on the risks provided, the options noted in the previous section are available.
- At this stage the HIA has to decide:
  - Which risks should be checked to ensure they are being properly managed?
  - When should they be checked (this year, next year)?
  - How should they be checked?
- These three questions are answered below. The 'how?' question is answered in greater detail in stage 3.
- The guidance below applies to organisations that are risk enabled or risk managed. Guidance is provided at the end of this stage for risk defined organisations.

> It is not possible to carry out risk based internal auditing without a reliable risk register, that is in organisations that are risk naïve or risk aware. Such organisations need to improve their risk maturity to a minimum of risk defined before RBIA can be used.

- The diagram below shows the main processes involved in this stage.

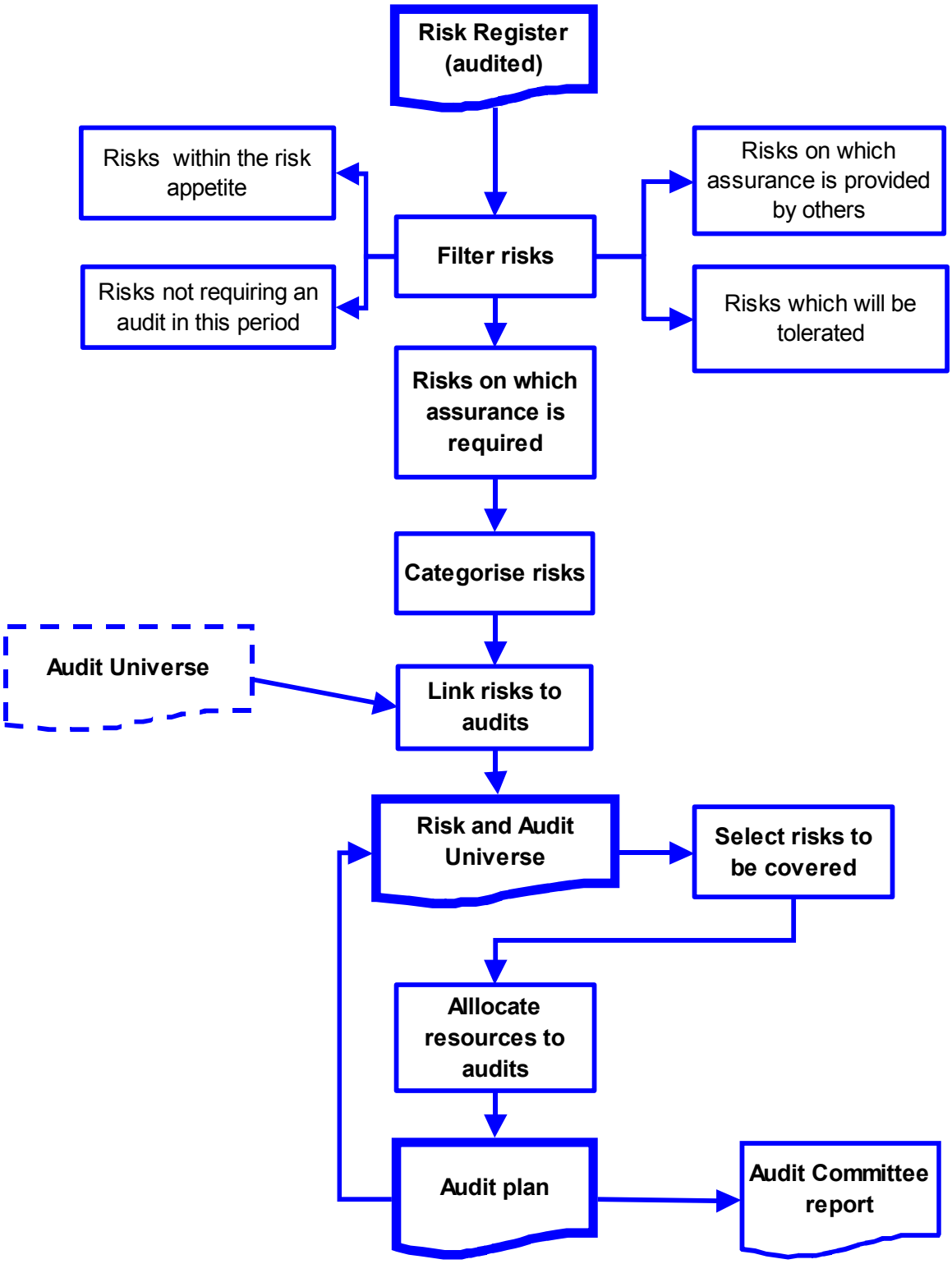


Fig 4 Processes involved in Stage 2

3.5.2 Aims of these stages

- To produce a 'risk and audit universe', which lists all risks and, where applicable, the audits that will provide assurance that the processes which manage risk are effective. An example format for the risk and audit universe is shown in appendix F.
- To produce an audit plan, listing audits to be carried out over a specified period, usually a year. This plan will include all the audits, and other work, which enable the internal audit department to report its conclusions on the risk management processes, as defined by the terms of reference agreed with the audit committee. An example audit plan is shown in appendix H.

3.5.3 Action to achieve these aims

The functions carrying out these tasks will depend on the structure of the organisation and Internal Audit's responsibilities.

3.5.3.1 Determine the risks requiring assurance

- Obtain the risk register (example in appendix B). Ideally this will include most of the risks above the risk appetite, plus others, scored by a standard system that has a defined risk appetite. The process of determining and scoring risks has been audited in stage 1 and it may have been necessary for the internal audit department to facilitate the compilation of the risk register.
- Filter the list of inherent risks to remove those where an audit is not possible or necessary, as follows (*audit action in brackets*):
  - The risk is within the risk appetite of the organisation and requires no further work. (*No audit*)
  - The nature of the risk is considered such that it cannot be bought within the risk appetite, and it will be tolerated. If contingency plans are required, do not filter out the risk, in order to ensure the plans are audited. (*Tolerate, consider auditing contingency plans*)
  - The risk is being examined by a third party (external auditors, quality control, health and safety), who may provide assurance directly to the audit committee, or through internal audit, or through another function (director of governance, for example). The organisation's overall strategy on assurance should provide guidance. (*No audit, assurance from …*)
  - The risk was being managed within the risk appetite, as evidenced by previous audit work. Taking into account the risk evaluation, audit results, management monitoring of controls, changes in the area concerned, and the time since the last audit, internal audit can provide assurance that risks will remain within the risk appetite, without doing any audit work. A date outside the plan may be recommended for the next audit. (*Assurance available. Next audit…)*
- The remaining risks are those on which assurance is required and these will form the basis of the audit plan. These risks, and those filtered out, will be included in the report to the audit committee, so they are aware of how *all* the risks are being managed. Note that risks where the response is *terminate* or *transfer* remain in the plan, in order to provide assurance that the appropriate action has been taken and the risks no longer exist, or are within the risk appetite. More details are included in the next section.

3.5.3.2 Allocate risks to audits.

- **Categorise the risks**. If there are a large number of risks, it will be useful to categorise them, if this has not been done. Categorising will group the risks into a logical order, which will assist in compiling the audit plan, especially where it is possible to audit the responses to several risks in one audit. Where there are a large number of risks, it also assists in preventing risks being duplicated, as they are likely to fall into the same category. The primary aim of categorisation is to aid the planning of internal audits, not select audits. That comes from the risks. Useful categorisations are:
  - **By objectives**. This links audits directly to the objectives threatened by the risks, whose management is being checked by the audit. It is therefore very useful when assessing the audit plan for its relevance to the organisation.
  - **By risk owner**. This method can be used for audits in specific locations, such as oil refineries.
  - **By business unit**. This is useful where the organisation has a number of physically independent business units, whose processes are self-contained. It may be necessary to duplicate risks (for example those arising from computers) across all the units.
  - **By process**, such as sales, purchases, stock control. This is useful in a large central organisation with integrated systems. An example Process Hierarchy is shown in appendix D. The Risk and Audit Universe (appendix F) uses processes to categorise and order risks.
  - **By type**, such as governance, financial, external, operational and compliance. These types are suggested in some UK Government documents. They are rather broad and also can overlap. For example, a failure to maintain adequate books and records is a financial and compliance risk.
- **Link risks to audits. There are two methods which can be used to link risks to the audits which will check their management:**
  - **Group the risks**, for example by business unit, objective or process, and decide the audits that will provide assurance on the management of these risk groups. This method has the advantage that the management of all risks will be checked but it may be difficult to define audit units which satisfy the organisation's preferences for audit 'size', for example the number of staff who usually work on an audit and for how long.
  - **Set up an Audit Universe** (appendix E), for example where each audit is allocated to a business unit or process, and assign the risks to be assessed to these audits. This method is used by some organisations because it has the advantages of covering one physical location in one visit and of allowing the definition of suitably sized audit units. It does require a check to ensure that the management of all the risks is being audited.
- The linking of risks to the audits which will provide assurance is a crucial stage, as it will determine the scope of the individual audits.
- Ensure that the management of those risks which may not be linked to processes or business units, such as external risks, are included in the audit plan.
- Where the response to risks is not treatment (controls), other action might be required. This is noted in the *Response* column:
  - Risks are tolerated: the audit committee should be aware of this and the possibility of providing assurance on contingency plans considered.

- Risks are transferred (for example by insurance): assurance should be provided that all risks are transferred and robust processes exist to ensure any appropriate new risks are captured. Where it is considered that risks have been outsourced, for example information system risks to a third party supplier, it will be necessary to identify the new manager of the risk and that any compensation for their failure to manage risks is adequate and set out in the contract.
- Risks are terminated: assurance might be necessary to confirm the risk has disappeared.

- Providing assurance on the management of some risks, such as a major disagreement among directors, may be considered impossible. However, this may mask a reluctance to address the risk, or put in place contingency plans. Every risk should have a response; every response can be audited.
- Consider the list of audits identified. Are there any missing that the internal auditor would consider essential to check the management of significant risks? Their absence may indicate that some risks are missing from the risk register.
- Each audit group (that is risks to be covered by the same audit) are given a unique identifier (the example uses letters A…Z, AA…AA, BA…BZ and so on). This enables the spreadsheet to be sorted on this column in order for risks to be grouped by audit.
- Risks and audits are now linked and the resultant list is known as the *Risk and Audit Universe* (appendix F). Further details of the columns are given in appendix G.

3.5.3.3 Small organisations

- In a small organisation, for example a small charity which has to produce a risk assessment by law, 'internal audits' will not be a realistic way to confirm risks are being managed.
- In these organisations the response to each risk can be checked individually, and the result noted against the risk in the *Risk Database*. An example of this type of database can been downloaded from www.internalaudit.biz.

3.5.3.4 Draw up the proposed annual audit plan

- **Selection of risks**. At this point the risk and audit universe shows risks, their scores and the audits linked to them. The audit approach, assurance or consultancy, has not been decided. This is done as follows:
- **Sort risks** by the inherent risk score and for those above the risk appetite:
  - If the control score is high (takes residual risk to the risk appetite or below) – assurance approach to confirm risks are being properly managed
  - If the control score is low (residual risk is above the risk appetite) – consultancy approach to facilitate management's identification, assessment, managing and monitoring of risks.
- **Selection of risks to be covered this year**. There will be a range of scores and, in drawing up the audit plan, a policy will have to be established about which risks to cover and how often. It is unlikely that the board, or audit committee, will require assurance on the management of every risk above the risk appetite, every year. They may require assurance on the risks with a high likelihood of significant/catastrophic losses every year but other risks above the risk appetite every two or three years. *Note the audit action to be taken and the next audit year in the appropriate columns*.

  The diagram below shows a possible method of assessing the type of work and frequency. The thick line represents the risk appetite (the equation of the line is control risk = inherent risk – risk appetite).

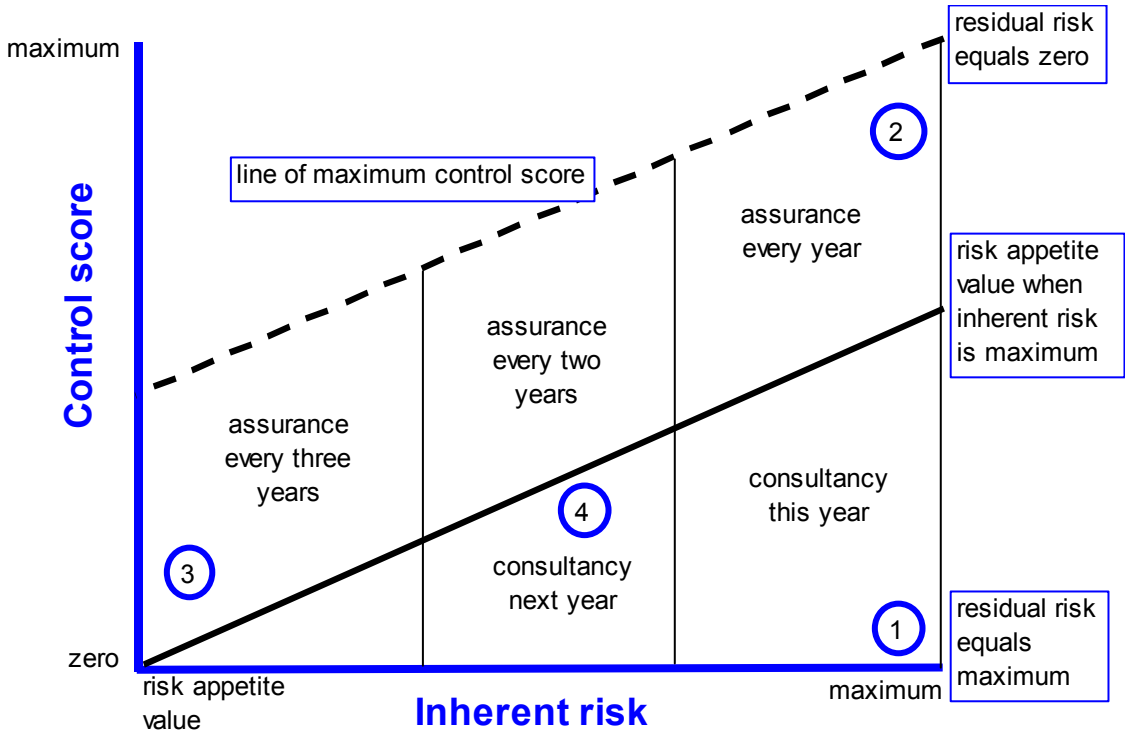


Fig 5 Frequency of Audits and Consultancy

Some example risks (1-4) are shown on the diagram:

1. Where the control score is near zero and the inherent risk is near the maximum possible value then the residual risk is very high. Consultancy work should be carried out with management to determine the improved response as soon as possible.
2. Where the inherent risk is near its maximum and the control score is very high, then the effectiveness of the risk management should be checked every year as the control is considered to be very effective.
3. Where the inherent risk is near the risk appetite, then the board may decide that assurance is not required every year.
4. Where the inherent risk is moderate and the control score is low, the residual risk will be above the risk appetite but may not be considered serious. In this case any consultancy work with management to reduce the risk can be done next year.

- **Audits to be planned**. At this stage the individual risks that are to be examined have been determined. Since the management of several risks is included in one audit, the audits may be prioritised by adding up the control scores of the risks included, for example. Priority would be given to assurance audits with the highest control scores and consultancy audits with the lowest control scores.

- **Additional audits.** All the audits to be included in the plan should have now been determined. However, many organisations like to add audits based on criteria other than risk. Such criteria might include: areas subject to change; mandatory audits; audits requested by management. However, these criteria should be reflected in the likelihood or consequence scores. For example, considerable change happening in an area could result in increases in the likelihood of a risk occurring. If an audit has to be included by management request, then it is displacing an audit included on the basis of risk scores and management should justify this substitution.

3.5.3.5 Allocate resources

- The number of days required to complete each audit is estimated. The total of days required to audit all the controls over the risks is summed and compared to the resources available. This calculation is included at the end of the audit plan (appendix H) and at the end of the RAU (appendix F).
- If resources are insufficient to complete the plan, prepared on the basis of internal audit's terms of reference, an increase in staff should be considered, alongside other options, such as reducing the number of audits.
- If sufficient staff are not available, the audit committee should be informed of those risks not audited due to resource constraints and given the opportunity to decide on their preferred option.
- When resources have been allocated, approximate timings and other details of the audit can be input to the RAU under the 'Next Audit' columns. A unique reference (separate from the audit group letters) is given to each audit and used on all audit documentation.

3.5.3.6 Publish the audit plan

- The audit plan can now be extracted from the Risk and Audit Universe, for example sorting by 'audit plan date' and copying the relevant audits to another spreadsheet. This should provide the audit committee with:
  - Details of those risks where assurance will be provided on the risk management processes, by carrying out the audits in the plan.
  - Details of those risks where assurance will be provided but based on audit work from previous years.
  - Details of those risks where consultancy work will be carried out to assist management in reducing the risks to below the risk appetite.
  - Any risks not covered, due to policy or resource constraints.
  - Confirmation that the plan is in accordance with the internal audit department's terms of reference.
- An example plan is shown in appendix H.

3.5.3.7 Update the risk and audit universe

This should be done regularly**,** at least every three months, from management's re-assessment of risks and conclusions from audits reporting during this period. The impact on the audit plan should then be considered. It may be necessary to add audits where new, significant risks have been identified and remove those where risks are considered to have diminished. In particular, it will be necessary to add new major projects to this list.

3.5.4 'Risk defined' organisations starting to use RBIA

- Where an organisation is only assessed as 'risk defined', it is likely to have most risks determined and scored, but not in a single list. There is also the possibility that some risks may be missing. While one of the internal audit's department's tasks may be to facilitate this, audits have to be carried out.
- The process here is to use management's assessment of inherent risk, with audit facilitating risk workshops to fill any 'gaps' in the risk register. High inherent risks can be linked to audits based on the existing audit universe, such as processes or business units.
- Once the risk register is complete, the above procedures can be used. Audits should be targeted at high inherent risks, as control scores may not be reliably known.
- Audit conclusions are likely to be a mix of assurance that risks are being managed and consultancy proposals to improve controls and monitoring based on discussions with management.

3.5.5 Risk aware and risk naïve organisations wishing to use RBIA

- Comprehensive RBIA depends on a risk management framework being available in an organisation and, in particular, on the existence of a complete risk register. Since these don't exist in risk aware and risk naïve organisations, the emphasis must be on internal audit promoting risk management, even to the extent of acting as project manager.
- In the short term, risk driven audits can be carried out using the methodology in section 3.6. Internal audit will have to facilitate management's identification of risk, which will involve training, risk workshops, interviews and questionnaires. Audits will therefore take longer to complete but have the advantage that they will spread an understanding of risk throughout the organisation. However, it will still be necessary for the board to devise a strategy that will establish a risk management framework.

3.6 What do I have to do? Stage 3 – carrying out an individual assurance audit

3.6.1 Introduction

- The purpose of an individual audit is to provide assurance that risks are being properly managed, and report where they are not.
- The audit plan is that part of the risk and audit universe which shows the audits to be carried out in the specified period (usually a year). It also shows the risks to be covered in any audit and may also provide details of personnel, budgeted time and estimated date for issue of the report.
- The plan may be used to generate a quarterly plan that provides greater detail about the staff working on the audit and how their time is to be used.
- The main tasks involved in an individual audit are shown below, with greater detail provided in the section for internal audit staff:

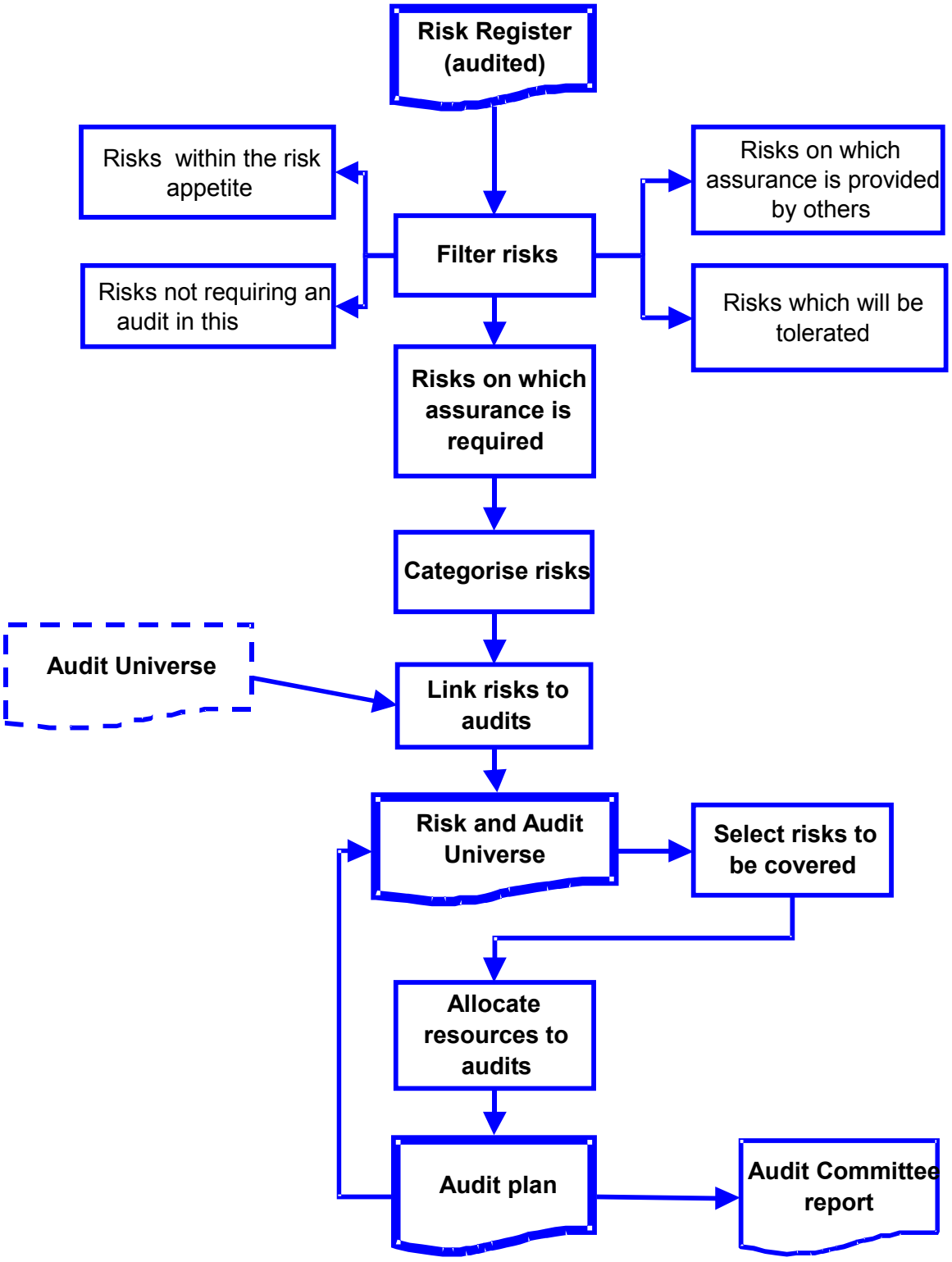


Fig 6 Processes involved in Stage 2

3.6.2 Aims of this stage

- The audit work should be able to provide assurance that:

  - Management have identified, assessed and responded to risks above the risk appetite.
  - The responses, especially the system of internal controls treating the risks, are effective in reducing the inherent risks to below the risk appetite.
  - Where residual risks are above the risk appetite, action is being taken to reduce them to within the risk appetite, or the board has been informed that they will be tolerated, transferred or terminated.
  - Risk management processes are being monitored by management to ensure they continue to operate effectively.

  The requirement for these conclusions is based on the Turnbull Guidance (paragraph 29), which requires that the board consider these when reviewing reports during the year. They are consistent with the five key internal audit roles in regard to ERM.

- For each of the risks covered, the audit should give reasonable assurance that:

  - The risk is being managed to within the risk appetite of the organisation or,
  - Action has been agreed to bring to the risk within the risk appetite or,
  - The risk will have to be tolerated or,
  - The risk is being terminated or transferred, or
  - The risk is not being managed to within the risk appetite, and no suitable action is being taken.

  The opinion on each risk will determine the assurance that can be given based on the complete audit.

- The results of the audit are used to advise management on updating the risk register with the actual status of the residual risks.

3.6.3 Action to achieve this aim

- **Anticipate the risk maturity**. The processes within an audit will vary according to the risk maturity of the organisation (determined in stage 1) and quality of risk management in the area concerned. The starting assumption should be that the risk maturity of the area to be audited is at least as good as the risk maturity of the organisation, and the expectation is in the table below. If audit work shows that this is not the case, the work plan will need to be changed to reflect this.
- **Determine the risk maturity.** The overall structure of a risk based internal audit, from the HIA's point-of-view is:
  - Confirm the scope of the audit with management.
  - Have staff assess the quality of risk management over the processes involved by talking to managers, finding out how they monitor controls, and examining evidence. Appendix A gives guidance on the criteria. This will determine the risk maturity of the area concerned, which may not be the same as the maturity for the organisation as a whole.
  - With the staff involved in the audit, conclude on the adequacy of risk management, consistent with the core internal audit roles in regard to ERM (details under 'Guidance for internal audit staff'). That the risk management process has, within reasonable assurance:
    - Identified all significant risks.
    - Correctly assessed all risks; that is scored and prioritised them.
    - Implemented appropriate responses to risks (tolerate, transfer, treat, terminate).
    - Reported significant risks to the board.
    - Established a robust system of monitoring internal controls.

- **Decide on the approach.** Depending on the above conclusions, decide on the audit approach (see section 3.4.3 and below). The diagram summarises the controls and monitoring present and the mixture of assurance and consultancy work necessary.

	Controls	Monitoring	Audit approach
Risk enabled	All risks identified and assessed. Regular reviews of risks. Responses are in place to manage risks	Management monitor that all types of response are operating properly. All managers provide assurance on the effectiveness of their risk management and are assessed on their risk management performance	Assurance
Risk managed		Management monitor that all types of response are operating properly. Most managers provide assurance on the effectiveness of their risk management and are assessed on their risk management performance	
Risk defined	Majority of risks identified and assessed. Regular reviews of risks. Responses are in place to manage most risks	Some management monitoring that all types of response are operating properly	Consultancy
Risk aware	Controls may be in place but are not linked to risks	Little monitoring	Cannot use RBIA. Adopt a consultancy approach to promote risk management and achieve 'risk defined' status. Carry out risk driven audits.
Risk naive	Controls, but some may be missing or incomplete	Very little, if any monitoring	

- Where areas concerned are **risk managed**, or **risk enabled**: detailed audit work is unlikely to find missed risks and deficient controls. The emphasis should be on auditing the risk management processes, for example resources, documentation, methods and reporting. Particular attention should be paid to verifying the management's monitoring of controls over key risks (those with a high control score).
- Where the area is **risk defined:** audit work will include verifying the risk management processes work effectively, but detailed audit work will be required to ensure all risks have been identified and tests carried out to ensure controls are operating.
- Where areas are **risk naïve or risk aware**, risk driven audits will be possible, but will require management training and risk workshops to determine risks in the areas concerned. Internal audit should not determine risks without management involvement, nor maintain their own list of risks. This will only reinforce management's belief that internal audit are responsible for risk management.

- **Carry out the audit (details under 'Guidance for internal audit staff')**
  - Carry out the audit work.
  - Discuss the issues raised with management and issue the audit report.
  - Update the risk and audit universe, after agreement with managers.
- **Summarise the audit conclusions for the audit committee.** The nature and timing of this summary will depend on the terms of reference governing the internal audit department. As a minimum this summary should:
  - Support the requirement of any regulations (Turnbull, Smith) that apply to the organisation.
  - Fulfil the requirements of the terms of reference.
  - If not part of the above, provide an opinion on whether risks are being managed sufficiently to ensure the organisation's objectives are being achieved and, within reasonable limits, will be achieved in the future.

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

3.7.1 Achieving targets

- The targets set for a Head of Internal Audit are likely to include:
  - Compilation of an audit plan that ensures the department fulfils its mandate from the audit committee, detailed in its terms of reference.
  - Gaining acceptance from management that they will take appropriate action to manage those risks found to be above the risk appetite.
  - Operating an effective internal audit function in the overall context of the organisation's risk management system (see the five core internal audit roles in section 3.2)
  - Keeping within the budget set for the department.
- The first three bullet points are based on paragraphs 4.10 and 4.12 of The Smith Guidance on audit committees, which details some of the responsibilities an audit committee should include in its review of internal audit's work. RBIA is essential to the achievement of these targets, in that:
  - The audit plan is based on risks (also required by the Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing*).
  - Internal audit's recommendations, where they are made as part of its consultancy role, are linked to risks determined by management and the processes which management should have in place to control them.
  - The work of internal audit is directly linked to the risk management system.

3.7.2 Audit resources

- RBIA can have another beneficial effect – it justifies 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 determine the audits that can be carried out. It also ensures that resources are directed towards checking the management of the most significant risks.

3.7.3 Relationship with management

- One major, positive, impact can be changes in the relationship with 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 serious weaknesses 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 internal audit departments:
  - The risks to be covered in audits will exist in all parts of the organisation and audits will therefore involve managers in departments never visited before. Many risks will be very significant to the organisation and the discussion of their controls will involve more senior managers and directors than might be involved in traditional finance orientated audits.

- RBIA emphasises 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.
- The HIA will be required to 'sell' the concept and need for internal audit. 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 programmes 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.

3.7.4 Management responsibility for risk management

➢ RBIA requires managers to face up to their responsibility for risks. It is easy for managers to compile a list of risks; it is a different matter to accept responsibility for them.

➢ In taking responsibility for risks, managers will understand that controls are not the responsibility of internal audit, and hence imposed by that department, but are their own responsibility.

3.7.5 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 programmes, 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.

3.7.6 Staff expertise

- The expansion of the audit universe to cover all risks threatening the organisation'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 assurance that 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 organisation's external auditors.
  - Recruit specialists from inside the organisation. 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 organisation. For example health and safety experts to audit an organisation'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.

3.7.7 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 programmes 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.

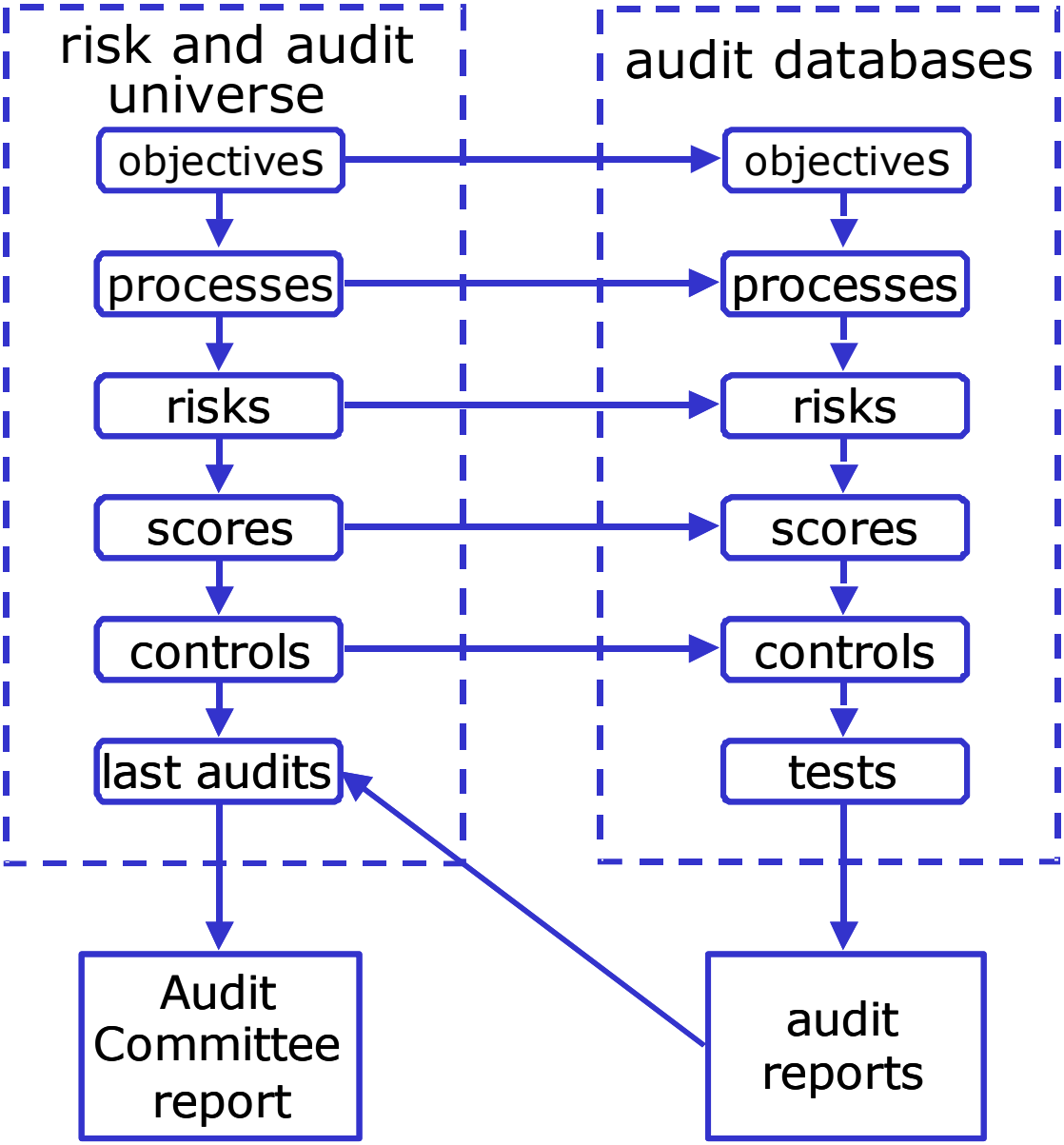


Fig 7 Audit trails in the risks and audit universe and audit

3.8 I've got some questions

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

Theoretically, not much. The IIA Standards require that audit plans are based on risk (Performance Standard 2010) and that audit engagements take risk into account (2201). In reality there may be a considerable difference, especially if the audit department is carrying out compliance audits, or those based on audit programmes. Such audits are usually confined to finance processes and will not cover many of the major risks threatening the objectives of the organisation. There is also a danger with audit programmes 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 programmes should therefore be abandoned!

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 authorised', is the absence of a control.

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

Why can't I just carry on as normal?

That depends on the organisation you work for and what 'normal' is. If your organisation is required to ensure its risks are being properly managed but the internal audit department is only carrying out financial audits using audit programmes, then you need to adopt RBIA for the reasons noted in this guideline. Even if you are in an organisation not required by regulations to manage risks, establishing a risk management framework and adopting RBIA will ensure internal audit resources are directed at those risks that have the potentially greatest impact on your stakeholders.

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 organisation'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. HIA 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 Head of Audit, needs to be read.

4.2 What is RBIA?

Risk Based Internal Auditing is the methodology that provides assurance that the risk management framework is operating as required by the board**.** RBIA not only involves risks in prioritising the annual audit plan but also in prioritising 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 head of internal audit considers how the risk maturity of the organisation will determine the audit approach. For internal audit staff, there are two approaches:

  - **Assurance**: The biggest difference from traditional audit work is that there is much less emphasis on, 'which controls are working?' and much more emphasis on, 'how does management monitor that controls are working?'
  - **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 section below details the work to be done in individual assurance audits, although the methodology should also be used for the consultancy approach when possible. The main difference between the two approaches is that the assurance audit will use information on risks, controls and monitoring which is already prepared, while the consultancy audit will involve facilitating the preparation of this information. The documentation can be the same.
- 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 programmes, 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 assurance that risks are being managed to an acceptable level (as determined by the risk appetite) or to facilitate and/or agree improvements as necessary.
- The diagram in stage 3 shows details of the processes.

- Much more detail on the methodology to be used is available from the internal audit manual on www.internalaudit.biz.

4.3.2 Maturity of the risk management processes

- **Draw up a draft scope**, basing it on the audit plan and the risks in the risk and audit universe.
- **Examine the risk management processes:**

  Use the audit questions in appendix A to determine the risk maturity of the area being audited.
- If considered necessary, **scrutinise the risks identified by management** to ensure they are complete. This can be done by an auditor competent in the area concerned, by an independent member of staff seconded to the audit, or by an external expert. If risks are missing, they should be found during the audit.
- **Conclude on the risk maturity of the processes being audited**. Do risk management processes exist to:
  - Identify all significant risks?
  - Correctly assess all risks, that is score and prioritise them?
  - Implement appropriate responses to risks (tolerate, transfer, treat, terminate)?
  - Report significant risks to the board?
  - Establish a robust system of monitoring internal controls?
- **Decide on the audit approach** based on the above conclusions. The options available and action to be taken will be discussed with the HIA and are included in section 3.4.3. The work to be carried out will depend on the risk maturity of the area. Where an individual audit is to be carried out the options are:
  - Risk management processes are acceptable: evaluate the processes and determine how management gain assurance that the risk management activities are being carried out as intended.
  - Risk management processes are unacceptable: facilitate risk identification and assessment to determine inherent risks, response and residual risks.

4.3.3 Testing and verification

- **Interview staff:** obtain documentation and carry out risk workshops, as necessary, to determine the detailed objectives and risks. The audit plan will have provided high-level risks; this task is to obtain more detail about the objectives and targets of the processes involved and the risks that threaten them. An example process map, for expense purchases, is shown in appendix G
- **Agree the scope of the audit with the managers involved**. The scope will include:
  - Reasons for the audit.
  - The objectives of the processes being audited.
  - The principal risks being audited (from the risks and audit universe) and other significant risks that have been mentioned during the discussion of the draft scope, or obtained from documentation.
  - The processes involved, and those specifically excluded.
  - Any special considerations, such as external auditor's findings, recent frauds, major system changes.

- The main stages of the audit.
- The staff involved, with their responsibilities, and time to be spent
- The primary client contact (sometimes known as the 'client sponsor')
- The timetable for the audit. Stating the expected dates of circulation for the draft and final reports, and who will receive them.

➢ **Obtain relevant documentation** on processes in sufficient detail to ensure:

- All the risks have been identified and assessed (scored) correctly by management against agreed standards. Use walkthrough tests as appropriate to confirm the processes. It is probable that these tests will identify new risks not previously identified by managers. In this event, agree the existence of the risks with management and facilitate their scoring.
- Controls that should be operating to manage the risks have been identified.
- Processes which management use to monitor the proper operation of controls have been identified
- Tests to check the effectiveness of the controls and monitoring can be defined.

➢ **Set up an audit database to record processes**, the risks that threaten them, controls, tests and conclusions. An example is shown in appendix H for an audit of expense purchases in a risk defined organisation. Depending on the audit software being used, these details may be added to a single database containing all risks. Small audit teams could use a spreadsheet.

➢ **Carry out the tests** to check whether the controls and management monitoring are effective. Where reliance is being placed on management's assessment of risk, the emphasis will be on ensuring the monitoring is taking place. In all circumstances, view evidence that controls are operating as expected and pay particular attention to controls with a high control score.

➢ **Assess management's scoring of the residual risks**, taking into account the controls actually in operation.

4.3.4 Reporting

➢ **Draw preliminary conclusions** on the effectiveness of the management of each of the risks. Figure 2 shows the relationship between the residual scores and the conclusion on the management of the risks. For each of the risks covered, the audit should give reasonable assurance that:

- The risk is being managed to within the risk appetite of the organisation (*acceptable*) **or**,
- The risk is not being managed within the risk appetite (*unacceptable, issue, supplementary issue*) **and**
- Action has been agreed to bring to the risk within the risk appetite or,
- The risk will have to be tolerated or,
- The risk is being terminated or transferred, or
- The risk is not being managed to within the risk appetite, and no suitable action is being taken.

➢ **List 'issues' for discussion with management** where residual risks are above the risk appetite. The combination of the opinion on each risk, and the level above the risk appetite, will determine the overall conclusions.

- **Discuss the results** with the appropriate people during the audit and in a meeting at the end of the fieldwork, noting action they will take to bring any risks within the risk appetite, or risks they will terminate, transfer, or tolerate. These last three risks should be included in the report and referred to senior management, or the audit committee, to ensure that they are satisfied the response is appropriate. Where risks are to be tolerated, check the existence, and testing, of any contingency plans.
- **Write and issue the draft report**, in order to obtain agreement on any recommendations, and the conclusions. The format of the report, and method of communication, will be defined by the organisation.
- Based on the conclusions against each risk, it will be possible to provide assurance that:

  - Management have identified, assessed and responded to risks above the risk appetite.
  - That the responses, especially the system of internal controls treating the risks, are effective in reducing the inherent risks to below the risk appetite.
  - That, where residual risks are above the risk appetite, action is being taken to reduce them to within the risk appetite, or the board has been informed that they will be tolerated, transferred or terminated.
  - Risk management processes are being monitored by management to ensure they continue to operate effectively.

  Or indicate why assurance cannot be given. Guidance on how to decide on the conclusion against each of the above points is provided in appendix J.
- **Write and issue the final report** having amended the draft report as necessary. Issue the final report to the parties defined by the Internal Audit Department's Charter.
- **Update the risk and audit universe**, after obtaining management agreement.

4.3.5 Documentation

The audit should be documented in such a way that:

- Evidence for the audit conclusions is complete and easily found.
- Issues can be easily traced back to the reasons, and evidence, for raising them and to the action being taken to address them.
- Risks, their controls, the audit tests and conclusions are linked in such a way that the conclusion on any risk can easily be found. The audit database is the key document to enable this.
- Important decisions from meetings are noted.

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 programmes 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 programmes, 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 organisation, 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 organisation.

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 authorising 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 organisation'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 organisation.

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, councillor or governor.

Enterprise-wide Risk Management (ERM): A structured, consistent and continuous process across the whole organisation 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 organisation 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 organisation 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 organisation 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 organisation 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.

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 organisation 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 organisation's objectives.

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

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

Risk Responses: The means by which an organisation 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 organisation 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 Further reading

(When this document is viewed on a computer, the underlined words are hyperlinks to the websites concerned)

6.1 Institute of Internal Auditors

- *Risk Based Internal Auditing*, Institute of Internal Auditors (UK and Ireland).
- *The Role of Internal Audit in Enterprise-wide Risk Management*, Institute of Internal Auditors (UK and Ireland).
- *An approach to implementing Risk Based Internal Auditing*, IIA UK and Ireland. Available from the site at IIA bookstore
- *The International Standards for the Professional Practice of Internal Auditing*, Institute of Internal Auditors Inc. Available from www.theiia.org.

6.2 UK Government standards and regulations

- *The London Stock Exchange Combined Code*, with the Turnbull and Smith Guidances. All these documents are intended for companies listed on the London Stock Exchange, the principles they set out apply to any organisation and are some of the most clear and concise available. The documents are available from www.frc.org.uk.
- *The Orange Book. Management of risk – principles and concept*. HM Treasury. This is a useful introduction to risk management for any organisation. Also available is a Risk Management Assessment Framework that can assist in defining the organisation's risk maturity. These are available as downloads from www.hm-treasury.gov.uk (use the search function).

6.3 Other guidance

- *The Risk Management Standard*, IRM, AIRMIC and ALARM. This is available from www.theirm.org and gives a good introduction to risk management.
- *ANZ Risk Management Standard (AS/NZS 4360:2004)*, Standards Australia and Standards New Zealand. This is the original standard, now revised. It can be obtained from www.standards.co.nz or www.standards.org.au
- *Enterprise Risk Management – integrated framework, COSO*. More details of this US standard are available from www.coso.org (look under *Publications*).
- *It's a risky business: a practical guide to risk based auditing*, CIPFA. Available from www.cipfa.org.uk/. Aimed mainly at public service organisations, this document provides considerable detail on risk management and risk maturity.
- *Implementing Turnbull – A Boardroom Briefing, Institute of Chartered Accountants in England and Wales*, provides a good practical approach to introducing risk to the boardroom of any organisation. It can be downloaded from www.icaew.co.uk. (search on *Boardroom briefing)*
- *Good practice checklist for assessing risk management in Higher Education Institutions* (http://www.hefce.ac.uk/finance/assurance/guide/checklist.doc) provides a checklist for assessing risk maturity.

7 Biography

David M Griffiths

In 1972, I finished my chemistry Ph.D. at Nottingham University and joined Price Waterhouse as a trainee accountant.

I qualified in 1976 and moved to the internal audit department of the Boots Company PLC, a retail chemists and healthcare company (£5bn turnover), before assisting in the introduction of inflation accounting.

I returned to be Head of the internal audit department a year later, in charge of 12 staff. Promotion to Head of Pharmaceutical Accounting Services followed, where I was responsible for 100 staff in payroll, fixed assets, accounts payable and accounts receivable departments.

Following the reorganisation of Accounting Services, I returned to internal audit, as Internal Audit Manager. During the last few years, I introduced risk based auditing into the department, using a database at its core similar to the Excel spreadsheet used on the website. This methodology was used for most audits, including computer and systems development audits.

I have now retired and am spending my spare time as a trustee for an almshouse charity and trying to keep my web site maintained! I was a member of the Institute of Internal Auditors (U.K.) Technical Development Committee and was involved in the writing of the Guidance Note on implementing RBIA. Hence the similarity of some of the appendices to those which have been on my site for some years. The views expressed in this book, and on the web site, are my own and are not endorsed by the Institute.

I have written a website on managing information (http://www.managing-information.org.uk/) and an article on auditing information for www.itaudit.org.

8 Appendices

Due to space constraints it is not possible to show full examples of the spreadsheets. These are available as a separate Excel file from www.internalaudit.biz .

The appendices are:

Appendix A	Scoring risks	Advice on the scoring of risks
Appendix B	Risk Register	An example risk register in the order of the processes in appendix D. In this risk map
Appendix C	Assessing risk maturity	Matrix giving the requirements for the five categories of risk maturity and suggested audit tests
Appendix D	Process map	An example process map for a company manufacturing and retailing
Appendix E	Audit Universe	List of all audits an organisation considers it requires to provide assurance on risk management. It is not essential, but assists those organisations wishing to ensure audits have particular characteristics, such as length of audit. It can only be considered complete when all risks have been assigned to audits, since some audits may be missing from the plan.
Appendix F	Risk and audit universe (RAU)	The complete list of scored risks and the audits that will check their management.
Appendix G	Column key	Details of the columns in the RAU
Appendix H	Audit plan	The audit plan derived from the RAU
Appendix I	Process map - purchases	An example process map for the processes used to procure any item for the organisation
Appendix J	Expense purchases database	The audit database used for the audit of expense purchases
Appendix K	Conclusions	Guidance for providing assurance on an individual audit

8.1 A – Scoring risks

If the consequence when the risk occurs is:	OR the likelihood of the risk occurring is:	Then the measure is defined to be:
A catastrophic impact on the organisation, threatening its existence Cash at risk> £1,000,000	Almost certain	**Catatrophic (5)**
To prevent the organisation achieving all, or a major part, of its objectives for a long time. Cash at risk <£1,000,000 >£100,000	Probable	**Major (4)**
To stop the organisation achieving its objectives for a limited period. Cash at risk <£100,000 >£30,000	Possible	**Moderate (3)**
To stop the organisation achieving its objectives for a limited period. Cash at risk <£30,000 >£5,000	Unlikely	**Minor (2)**
To cause minor inconvenience, not affecting the achievement of objectives Cash at risk <£5,000	Rare	**Insignificant (1)**

Values are examples ONLY and must be defined by the board of the organisation concerned

8.2 B – Risk Register (part)

Business unit	Process	Process Description	Key risk to process	Process owner	Cons	Like	Score	Resp	Control (examples)	Monitoring (examples)
Merchandising	Define objectives for selling goods	The objectives of the processes for selling are defined	The objectives will not deliver the organisation's objectives effectively and efficiently	Merchandise Director	5	5	25	treat	Overall targets for sales and profits are set by the board in the annual budget. As part of the budget package the Merchandise Director outlines the action to be taken to achieve the targets. See also strategy controls	Monthly reports of sales and profits are presented to the Board, with an explanation of variances
Merchandising	Sell in stores	Sell goods in stores operated by the organisation, or franchised	Fail to stock goods which the customers want to buy	Merchandise Director	5	5	25	treat	Regular visits by Merchandising Director and staff to markets which anticipate ours e.g. the US. Attendance at trade shows. Focus Groups	Quarterly presentation to Board by Merchandising Director on market trends
Merchandising	Sell in stores	Sell goods in stores operated by the organisation, or franchised	Fail to anticipate the competitions' initiatives to take a bigger market share	Merchandise Director	5	5	25	treat	All competitors' advertising campaigns are monitored, with a weekly report to the Merchandising Director.	None
Merchandising	Sell in stores	Sell goods in stores operated by the organisation, or franchised	Prices are not competitive	Merchandise Director	5	5	25	treat	Competitors' prices are monitored every week, with reports going to appropriate Heads of Merchandise Departments	None
Merchandising	Sell in stores	Sell goods in stores operated by the organisation, or franchised	Store layout confuses customers	Merchandise Director	4	4	16	treat	None	None

8.3 C - Assessing the organisation's risk maturity

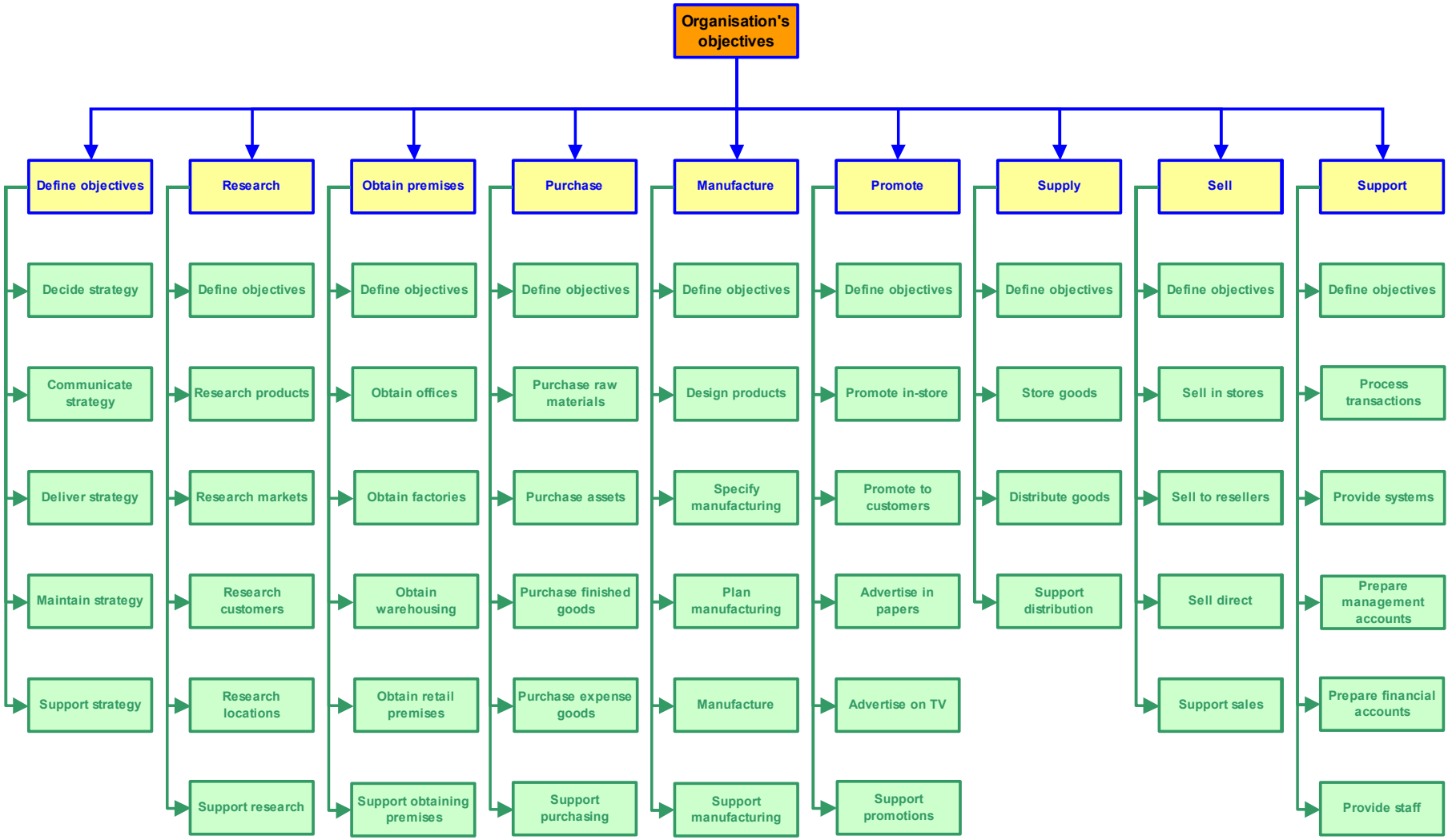
(A more detailed matrix is included in the IIA Guidance Note – An Approach to Implementing Risk Based Internal Auditing)

	Risk naïve	Risk aware	Risk defined	Risk managed	Risk enabled	Audit test (core IA roles in brackets)
Key characteristics	No formal approach developed for risk management	Scattered silo based approach to risk management	Strategy and policies in place and communicated. Risk appetite defined	Enterprise approach to risk management developed and communicated	Risk management and internal controls fully embedded into the operations	
Process						
Are the organisation's objectives defined?	No	In part		Yes		Check the organisation's objectives are determined by the board and have been communicated to all staff. Check other objectives and targets are consistent with the organisation's objectives. (1)
Have management have been trained to understand what risks are, and their responsibility for them?						Interview managers to confirm their understanding of risk and the extent to which they manage it. (1)
Has a scoring system for assessing risks been defined?						Check the scoring system has been approved, communicated and is used. (2)
Have processes been defined to determine risks, and these have been followed?						Examine the processes to ensure they are sufficient to ensure identification of all risks. Check they are in use, by examining the output from any workshops. (1)
Have all risks been collected into one list? Have risks been allocated to specific job titles?						Examine the 'Risk Universe'. Ensure it is complete, regularly reviewed, assessed and used to manage risks. Risks are allocated to managers. (1)

	Risk naïve	Risk aware	Risk defined	Risk managed	Risk enabled	Audit test (core IA roles in brackets)
Have all risks been assessed in accordance with the defined scoring system?	No	In part	In part	Yes	Yes	Check the scoring applied to a selection of risks is consistent with the policy. Look for consistency (that is, similar risks have similar scores). (2)
Have responses to the risks (e.g. controls) been selected and implemented?						Examine the risk register to ensure proper controls should be in place. (3)
Have management set up controls to monitor the proper operation of key controls?						For significant risks, examine the control(s) treating it and ensure management would know if the control failed. (5)
Are risks regularly reviewed by the organisation?						Check for evidence that a thorough review process is regularly carried out. (1)
Has the risk appetite of the organisation been defined in terms of the scoring system?						Check the document on which the controlling body has approved the risk appetite. Ensure it is consistent with the scoring system and has been communicated. (1)
Have management reported risks to directors where responses are not managing the risks to a level acceptable to the board?						For risks above the risk appetite, check that the board has been formally informed of there existence. (4)
Are all significant new projects routinely assessed for risk?						Examine project proposals for an analysis of the risks which might threaten them. (1)
Is responsibility for the determination, assessment, and management of risks included in job descriptions?						Examine job descriptions. Check the instructions for setting up job descriptions. (1)

	Risk naïve	Risk aware	Risk defined	Risk managed	Risk enabled	Audit test (core IA roles in brackets)
Do managers provide assurance on the effectiveness of their risk management?	No			In part	Yes	Examine the assurance provided. For key risks, check that controls and the management system of monitoring, are operating.(4)
Are managers assessed on their risk management performance?						Examine a sample of appraisals for evidence that risks management was properly assessed for performance. (1)
Internal Audit approach	Promote risk management and rely on audit risk assessment	Promote enterprise-wide approach to risk management and rely on audit risk assessment	Facilitate risk management/liaise with risk management and use management assessment of risk where appropriate	Audit risk management processes and use management assessment of risk as appropriate	Audit risk management processes and use management assessment of risk as appropriate	

8.4 D - Process map (part)



8.5 E - Audit universe (part)

Business unit	Last audit number	Next audit number	Next audit name	Next audit budget	Next timing	Next auditor	Status	Next final report Target
Merchandising		200	Selling strategy	10	Jan-06	Smith	To start	18-Jan-06
Merchandising		201	Market anticipation	20	Jan-06	Khan	To start	18-Feb-06
Merchandising		201	Market anticipation	(see above)				
Merchandising		203	Store planning	15	Mar-06	Smith	To start	24-Mar-06
Merchandising		204	Price file maintenance	20	Apr-06	Heath	To start	TBA
Merchandising	143	205	Stock control	22	Sep-06	Khan	To start	TBA
Merchandising		206	Store accounts	10	Jun-06	Smith	To start	TBA
Merchandising		202	Pricing policy	20	Feb-06	Heath	To start	27-Feb-06
Merchandising		207	Complaints procedures	30	Jul-06	Heath	To start	TBA
Payroll accounting services			Payroll					
Property			Geographic research					
Property	210	253	Location strategy		Jones	To start	20/08/2005	
Property			Locating offices					
Property			Locating factories					
Property			Locating warehouses					
Property			Locating shops					
Public relations			Communications					

8.6 F - Risk and audit universe (part)

Key risk to process	Response	Control (examples)	Monitoring (examples)	Cons	Like	Score	Control score	Audit action	Next audit number	Next audit name	Next timing
The objectives will not deliver the organisation's objectives effectively and efficiently	treat	Overall targets for sales and profits are set by the board in the annual budget. As part of the budget package the Merchandise Director outlines the action to be taken to achieve the targets. See also strategy controls	Monthly reports of sales and profits are presented to the Board, with an explanation of variances	5	1	5	20	audit	200	Selling strategy	Jan-06
Fail to stock goods which the customers want to buy	treat	Regular visists by Merchandising Director and staff to markets which anticipate ours eg the US. Attendence at trade shows. Focus Groups	Quarterly presentation to Board by Merchandising Director on market trends	5	1	5	20	audit	201	Market anticipation	Jan-06
Fail to anticipate the competitions' initiatives to take a bigger market share	treat	All competitors' advertising campaigns are monitored, with a weekly report to the Merchandising Director.	None	5	3	15	10	consultancy	201	Market anticipation	
Prices are not competitive	treat	Competitors' prices are monitored every week, with reports going to appropriate Heads of Merchandise Departments	None	5	2	10	15	consultancy	202	Pricing policy	Feb-06
Store layout confuses customers	treat	None	None	4	4	16	0	consultancy	203	Store planning	Mar-06
Prices are incorrect	treat	Retail prices are input by an assistant buyer and checked by a supervisor. Prices are downloaded onto the EPOS system overnight	A gross profit exception report is generated for any changes to GP >5%. This should pick up any incorrect input of retail prices. The report is signed off by a buyer.	4	1	4	16	audit	204	Price file maintenance	Apr-06

8.7 G – Column Key

COLUMN	Contents of cells		COLUMN	Contents of cells
L1	Level 1 risk number. Corresponds to the Risk database	**Last audit**	**Last audit number**	Unique number given to each audit. This is the number of the last audit to cover this risk
Level 1 process	Name of process		**Audit name**	Name given to the audit
L2	Level 2 risk number. Corresponds to the Risk database		**Last audit Budget**	Approximate number of auditor-days the audit should take. This aids resource planning
Level 2 process	Name of process		**Last audit actual**	Number of days the last audit actually required
L3	Level 3 risk number		**Last timing**	Months/year of last audit
Level 3 process	Name of process		**Last auditor**	Names of principal auditors
Process	Title of the process		**Last final report Target**	Target date for producing report (from scope)
Process Description	A brief description of what the process does. Any more details should be filed in the audit file		**Final report achieved**	Date actually achieved for issuing final report
Risk	The threat to the process. There may be several risks to one process, or one risk may threaten several processes		**Last result**	Conclusion of last audit (acceptable/issues/unacceptable)
Risk source	Who identified the risk (management, risk workshop, auditor, meeting)	**Current/Next audit**	**Audit plan date**	The date of the audit plan which includes the next audit (for example 2006/7)
Process owner	Job title of the person responsible for ensuring the risk is controlled and therefore for the monitoring controls		**Next audit number**	Unique number given to each audit. This is the number of the next audit to cover this risk - if it has been allocated
IRC	Inherent risk consequence score		**Next audit name**	Audit name. Will usually be the same as for the last audit, but could be different if this risk has been included in another audit

IRL	Inherent risk likelihood score
IRS	Inherent risk scores multiplied. (Inherent Risk Significance score)
Response	Tolerate, Terminate, Transfer, Treat
Control	Direct response to the risk
Monitoring control	Management's response to ensure the control is operating properly
RRC	Residual risk consequence score.
RRL	Residual risk likelihood score
RRS	Residual risk scores multiplied
Audit Group	Letter(s) given in order to group several risks into one audit (if necessary). They will not necessarily be in order, as new risks, with associated audits, will be added and some may be removed
Control score	Inherent Risk Significance minus Residual Risk Significance scores
Audit action	Audit; no audit (risk below risk appetite); assurance available from last audit; consultancy (residual risk above risk appetite); not covered due to lack of resources, etc.

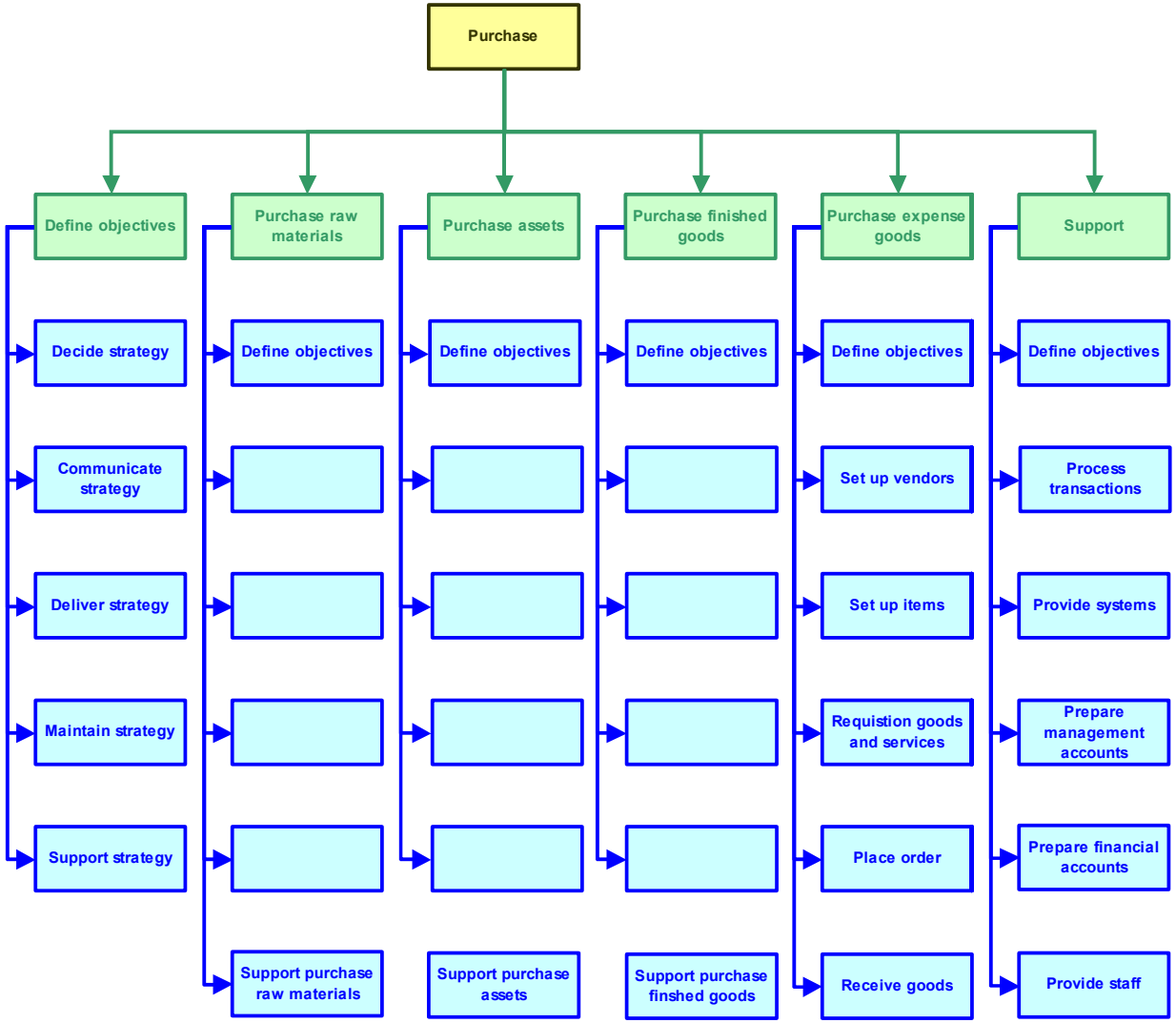
Current/Next audit

Next audit Budget	Approximate number of auditor-days the audit should take - based on last audit's actual time. This aids resource planning
Next timing	Expected quarter/year of next audit - if it can be allocated
Next auditor	Name|(s) of auditors - if allocated
Status	Status of audit (Planning/fieldwork/reporting) when it is in progress
Next final report target	Target date for producing report (from scope)
Next final report Achieved	Actual date the final report was issued
2006 opinion on risk	The opinion as to whether the risk was being properly managed

8.8 H - Audit plan (April 2005 – March 2006)

Business unit	Process	Audit plan date	Next audit number	Next audit name	Next audit budget	Next timing	Next auditor	Status	Next final report Target	Next final report Achieved	2006 opinion on risk
Merchandising	Define objectives for selling goods	2006	200	Selling strategy	10	Jan-06	Smith	To start	18-Jan-06		
Internet sales	Sell direct	2006	201	Internet sales	14	Oct-06	Heath	To start	TBA		
Merchandising	Sell in stores	2006	202	Pricing policy	20	Feb-06	Heath	To start	27-Feb-06		
Merchandising	Sell in stores	2006	203	Store planning	15	Mar-06	Smith	To start	24-Mar-06		
Merchandising	Sell in stores	2006	204	Price file maintenance	20	Apr-06	Heath	To start	TBA		
Merchandising	Sell in stores	2006	205	Stock control	22	Sep-06	Khan	To start	TBA		
Merchandising	Sell in stores	2006	206	Store accounts	10	Jun-06	Smith	To start	TBA		
Merchandising	Sell in stores	2006	207	Complaints procedures	30	Jul-06	Heath	To start	TBA		
Marketing	Sell to resellers	2006	207	Complaints procedures	(see above)						
Internet sales	Sell direct	2006	207	Complaints procedures	(see above)						

8.9 I – Process map for purchases (part)



8.10 J - individual audit database for expense purchasing (part)

Process	Process Description	Risk to process	Example control	Example monitoring	Tests	Issue
Define the strategy for expense purchasing	Set down targets for the year(s) ahead, for example, meeting the budget, improving staff efficiency, handling more orders	The strategy does not maximise efficiency and effectiveness and is not consistent with the organisation's strategy	The strategy for purchasing expense goods and services is updated each year, prior to setting targets and budgets for the areas concerned. These targets and budgets are approved by management finance.	Directors check the strategy for departments under their control. The overall budget is approved by the board	Examine the latest strategy document	None – an approved strategy exists
Deliver the strategy	Form an action plan, with the staff involved, to deliver the strategy	Any member of staff can authorise the purchase of any goods or services	Rights to place requisitions and orders are in a written policy	The policy is checked every year to ensure it is correct	Examine the policy. Check it is up-to-date, appropriate staff have a copy and know how to use it. As part of other tests, ensure adherence to the policy	Issue – some new staff are not aware of the strategy as it was omitted from their induction training
Set up Suppliers	Set up new Suppliers on the computer system, or modify existing details. Includes addresses and payment terms	Supplier details are not correctly input/modified	Details of all changes to the Supplier master file are printed on a report which is checked to supporting documentation by staff who are not involved in changing Supplier details	Details of Suppliers and the amount spent with them are printed out every six months for authorisation by the Purchasing Director	Check individual reports over the last six months for evidence of checking. Observe the process in action.	Issue – no evidence of the check on the reports
Set up Suppliers	Set up new Suppliers on the computer system, or modify existing details. Includes addresses and payment terms	False Suppliers are set up and paid	Details of all changes to the Supplier master file are printed on a report which is checked to supporting documentation by staff who are not involved in changing Supplier details	Details of Suppliers and the amount spent with them are printed out every six months for authorisation by the Purchasing Director	Check individual reports over the last six months for evidence of checking. Observe the process in action.	Issue – no evidence of the check on the reports

8.11 K – Guidance on assigning audit conclusions

Conclusion on:	Criteria		
Risks have been identified, evaluated and managed	Thorough processes have been used and all significant risks should have been identified.	Processes have been used, but there are some deficiencies and not all significant risks may have been identified.	Inadequate, or no, processes have been used.
Internal controls reduce risks to acceptable levels (that is to within the risk appetite of the organisation)	Risks are being managed to within acceptable levels, as defined by the board. **Report as** Supplementary issue, if cost effective controls can reduce the risk further, otherwise do not report	Not all risks are being managed to within acceptable levels, as defined by the board, although the consequence from the risk occurring, or likelihood of the risk occurring, is not considered significant. There is the possibility that some objectives will not be achieved **Report as**: Key issue	The risk is not being mitigated to an acceptable level by the control(s) and it is probable that some objectives will not be achieved, with significant (material) results (red) or The risk is not being mitigated to an acceptable level by the control(s) and objectives are not being achieved, with significant results **Report as**: Key issue
Action being taken to promptly remedy significant failings or weaknesses	The action being taken will result in all risks being managed to within acceptable levels.	The action being taken will result in some reduction in risk but not to acceptable levels	No action is being taken, OR insufficient action is being taken to manage risks to within acceptable levels
Current levels of monitoring are sufficient	No more monitoring is necessary than is done at present	Some additional monitoring is required	Major improvements are required to the monitoring of controls
Colour:	green	amber	red
Grading:	Acceptable	Issues	Unacceptable

Version control

Version number	Date issued	Changes made to previous version
1.0.0	30-Jan-2006	Issue of first version

9 Questionnaire

All information provided will be treated in the strictest confidence.

Size of organisation – turnover, or equivalent: £

Size of dept (all audit staff including managers)

Type of organisation (ring): Stock Exchange listed; private company; building society, educational establishment, health, government department, local authority, charity, other please state:

Country in which your organisation is primarily based:

What do you consider to be the risk maturity of your organisation (ring):

naïve; aware; defined; managed; enabled

At what stage do you consider RBIA is in your organisation:

Not started; used only for individual audits; not planning; implementing it; first year of implementation; experienced

On a scale of 1 to 4 (1=poor; 2=below average; 3=better than average; 4=good), please indicate your opinions of the following:

Overall opinion of the book:

Structure (division into parts addressed to directors, heads of audit, auditors):

Informal language used:

Examples of risk register and audit plan:

The practicality of the guidance given:

Do you agree that the document is necessary?: essential; useful; no use

Was the guidance: too simple; just right; too complex

What did the guidance do well?

What was omitted from the guidance?

What do you agree with in the book?

What do you disagree with in the book?

On what other subjects would you like to see book provided?

Please return this questionnaire to:

david@internalaudit.biz

Final, blank page