

Risk based internal auditing

**An
introduction**

**David
Griffiths**

PhD FCA

www.internalaudit.biz

**15 March
2006
Version 2.0.3**

Contents

Biography – David Griffiths

Introduction

- 1 Why does internal auditing exist?
 - 1.1 What's its main aim?
 - 1.2 So we've got risks?
 - 1.3 How do we manage risks?
 - 1.4 Who's responsible for risks?
 - 1.5 Where does internal auditing fit in?
 - 1.6 Where does 'risk management' fit in?
 - 1.7 Summary

- 2 Does it have to exist?
 - 2.1 Who says so?
 - 2.2 London Stock Exchange
 - 2.3 The Turnbull guidance
 - 2.4 The Smith guidance
 - 2.5 Sarbanes-Oxley
 - 2.6 PCAOB
 - 2.7 The Institute of Internal Auditors
 - 2.8 Management
 - 2.9 Summary

- 3 How does internal auditing find risks?
 - 3.1 The role of internal audit
 - 3.2 The role of management
 - 3.3 Finding and evaluating all the risks
 - 3.3.1 Finding risks and controls - an example
 - 3.3.2 The elements
 - 3.3.3 Objectives and processes
 - 3.3.4 The process map
 - 3.3.5 The elements
 - 3.3.6 Before or after internal controls?
 - 3.3 What risks are we prepared to accept?
 - 3.4 Finding the significant risks
 - 3.4.1 Start at the top
 - 3.4.2 Interviewing
 - 3.4.3 Risk workshops

RBIA – An introduction - contents

- 3.4.4 The accounts
- 3.5 Recording the risks
 - 3.5.1 What we've got so far
 - 3.5.2 The risk register
 - 3.5.3 Updating the register
- 3.6 Life in the real world
 - 3.6.1 Levels of risk maturity
 - 3.6.2 The impact of risk maturity

- 4 RBIA - the foundations
 - 4.1 What is risk based internal auditing?
 - 4.2 The organisation's requirements
 - 4.3 The RBIA stages
 - 4.4 The RBIA documentation
 - 4.4.1 The risk and audit universe (RAU)
 - 4.4.2 The audit database
 - 4.4.3 Other important documentation
 - 4.4.4 Summary
 - 4.5 Stage 1 – reliability of the risk register
 - 4.5.1 Objective of this stage
 - 4.5.2 Internal audit work
 - 4.5.3 Opinion
 - 4.6 Stage 2 – Compiling the risk and audit universe
 - 4.6.1 Objective of the stage
 - 4.6.2 Which risks?
 - 4.6.3 Grouping risks into audits

- 5 Compiling the audit plan
 - 5.1 Objective of the stage
 - 5.2 Why an annual plan?
 - 5.3 When to audit?
 - 5.4 Which audits?
 - 5.5 Resources
 - 5.6 The ongoing risk and audit universe
 - 5.7 Publishing the annual plan
 - 5.8 Quarterly plan

- 6 Providing the opinion
 - 6.1 Objective of the stage

RBIA – An introduction - contents

- 6.2 What is an audit?
- 6.3 Planning – the audit scope
- 6.4 Fieldwork - fact finding and risk assessment
 - 6.4.1 Risk maturity
 - 6.4.2 Ascertaining controls
- 6.5 Fieldwork - testing controls
- 6.6 The opinion
- 6.7 Reporting to management
 - 6.7.1 Update reports
 - 6.7.2 The close down meeting
 - 6.7.3 The report
- 6.8 Projects
- 6.9 Stage 5 – Report to the audit committee

- 7 What is the impact of risk-based auditing?
 - 7.1 How the delivery of internal auditing is changed
 - 7.2 Relationship with management
 - 7.3 Management responsibility for risk management
 - 7.4 Management of the department
 - 7.5 Staff expertise
 - 7.6 The benefits
 - 7.7 Disadvantages
 - 7.8 Some questions

- 8 Glossary

- 9 Useful information
 - 9.1 Audit and accountancy institutes
 - 9.2 Official standard setting organisations US
 - 9.3 Official standard setting organisations UK
 - 9.4 Risk management
 - 9.5 Other sites
 - 9.6 Sites with internal audit links
 - 9.7 Sites offering software and/or consultancy
 - 9.8 Books

- 10 Appendices
 - Questionnaire

David M Griffiths

Biography

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 manager 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. 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.

Introduction

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

I won't claim that my ideas are shockingly original, indeed most are built on accepted thinking and practices. Thanks are due to my colleagues in the Boots Group and contacts gained from the IIA-UK and Ireland for their help and advice – but the views expressed are my own. My aim in this book is to simplify some of the principles in internal auditing and make them consistent, based on risk.

This book builds on these principles to consider why internal auditing can be of benefit to an organisation and then details how, using risk-based methods, it can deliver this benefit.

This introduction is aimed at anyone interested in internal auditing, from Audit Committee members to students. It is split into chapters. The first two deal with the principles of internal auditing and should be of interest to all readers. The remaining chapters show how to introduce risk based internal auditing into an organisation and are more suited to readers who have some experience of internal auditing. Chapter nine provides links to useful web sites and should be of interest to all.

Internal auditing is related to both corporate governance and risk management. Corporate governance includes internal auditing and I have not covered other aspects of it in this book. I have covered risk management, but only as it affects internal auditing. The last chapter provides links that will give more information on these topics.

I should mention that this book discusses the objectives of internal auditing as a 'process' within an organisation, and *not* the objectives of an internal audit activity (internal audit department). Hopefully, the primary objective of an internal audit activity will be to achieve the objectives of internal auditing, but other aims may also involve documenting controls, stock counting, providing staff on secondment, routine branch audits and efficiency audits.

This book, with its related web site and audit manuals are my view of risk based internal auditing. They are not meant to represent 'best practice' but to be thought provoking. This book is not intended to be a lengthy, well-researched academic treatise, but a simple introduction. I've therefore used an informal, as opposed to an academic, style. I'll leave you to judge whether this works. I have written another book (available on www.internalaudit.biz) on the implementation of RBIA that is more formal and expresses more of a mainstream view, but not completely.

Finally, this book is copyright. I don't mind you using parts of it, provided you quote this source. It should not be used to promote any product or service, without my permission. I do mind you making money out of it, unless I get some!

Many thanks and happy reading...

1 Why does internal auditing exist?

1.1 What's its main aim?

Well, the *main* aim of any activity in an organisation should be to achieve the objectives of the organisation itself. Thus:

The main aim of internal auditing is to assist the organisation to achieve its objectives.

So if the organisation's objective is to 'add shareholder value' then that is the aim of internal auditing. If it is to 'Relieve famine in central Africa', then that is what internal auditors should be doing. Seems obvious, but it's worth making the point that internal auditing is not special. It should be able to justify its existence just like any other process in the organisation.

There is an assumption, hopefully justified, that the objectives of any organisation would include the requirement to obey applicable laws and regulations.

So how do internal auditors justify their salary? Let's go back to the objectives of the organisation. The achievement of these objectives is hindered by risks. Risks are what internal auditing is all about.

1.2 So we've got risks?

What is a risk? My definition:

A risk is a set of circumstances that hinder the achievement of objectives.

So, if our objective is to provide famine relief in central Africa, circumstances hindering this objective might be that we had no drivers for the lorries which transport the food.

An alternative way of defining risk is in terms of the chance of the risk occurring and its impact. For example, the ISO (International Standards Organisation) defines a risk as 'the combination of the probability of an event and its consequences' (ISO/IEC Guide 73). I prefer my definition, since the ISO one is not much help if we're trying to feed the starving with no food.

My definition also requires the existence of *objectives*. If we don't have any objectives – we don't have any risks. It also results in an interesting observation: that the same set of circumstances can be an opportunity, or a risk, depending on our objectives.

For example: take a farmer with land near the River Nile and a Curator managing a nearby museum. One objective of the farmer is to work fertile land, helped by the annual flood, which deposits river silt. One objective of the Curator is to keep the exhibits in his museum safe. The flooding of the Nile is therefore a risk to the curator, but an opportunity for the farmer. So if you don't know your objectives, you aren't going to get far in managing your risks.

1.3 How do we manage risks?

There are a number of ways the organisation can manage risks to bring them to a level which the board consider acceptable:

- Avoid the risks, for example not starting up a business selling innovative products or closing a factory making dangerous chemicals. This may mean giving up significant opportunities. This process is known as 'termination'.

RBIA – Why does internal auditing exist?

- Transfer them, the best example being insurance.
- Tolerate them, without planning any contingencies. These are the ‘asteroid hits earth’ type of risk. This does not mean that no-one will address this risk – governments may decide to try and deflect asteroids using nuclear missiles.
- Tolerate them, and plan contingencies. These are the ‘hurricane destroys factory’ type of risk.
- Introduce some processes to reduce the consequence or likelihood of a risk. These processes are usually referred to as ‘controls’ and include everything from having a clear strategy to installing a fire alarm. This method of management is known as ‘treatment’.

However, we will define any process which manages risk in one of the above ways as an ‘internal control’. Thus:

An internal control is a process which manages a risk.

This use of the phrase ‘internal controls’ is consistent with that used by the UK Treasury in its book ‘The management of risk – principles and concepts’. Also known as the ‘Orange Book’. It’s well worth reading (see chapter 9).

I don’t like the phrase ‘internal controls’ as it is used traditionally by accountants and auditors to describe controls in financial systems. Finding lorry drivers reduces a risk but doesn’t really fit the description of an ‘internal control’. However, we’ve got the phrase, so let’s stick with it.

It’s often said that’s risks are not always unwanted. For example, launching a new product is considered as a risk, although not an unwanted one. I don’t agree, launching a new product is a *process* with risks threatening its success. That doesn’t mean we don’t launch the product; it does mean we aim to reduce the risks to levels we can accept, which would at least be to a level where we can reasonably expect the product to make a profit! So we should aim at managing *all* risks. Ideally, we should try and quantify risks threatening projects, for example by using financial risk modelling. In this way the risks can be compared with the potential benefits.

Risks are also a fact of life. Some managers would like to remove them completely, but this is impossible without closing down the entire organisation (which also presents risks). So they need to be managed by internal controls.

There’s an important point about controls: *controls are a response to risk*. No risk, then you don’t need a control. In other words, controls are part of an organisation’s risk management framework, not the other way round.

1.4 Who’s responsible for risks?

So, our *objectives* are threatened by *risks*, which demand a response to avoid them, accept them, transfer them or treat them. Who’s responsible for ensuring that the response is appropriate to manage risks to a level that our controlling board can accept?

The various rules and regulations (more on these later) make it clear – the *management* of an organisation are responsible for:

- Identifying what risks exist.
- Assessing the risks.
- Ensuring that there is an appropriate response to all risks.
- Informing the board about risks which are outside acceptable levels (usually those which are to be tolerated or taken for the potential benefits)

RBIA – Why does internal auditing exist?

- Assuring the organisation's executive that it is monitoring the system of internal control which brings the remaining risks to within acceptable levels.

1.5 Where does internal auditing fit in?

Just as external auditors independently report on an organisation's accounts, so the internal audit activity independently reports that internal controls are operating properly. Recent financial scandals have reinforced the need for this type of independent opinion.

So what is the purpose of internal auditing? It is frequently phrased in terms like, "to ensure proper internal controls exist". The problem with this statement is that it gives the impression that internal auditing is only concerned with financial controls. Also, managers frequently consider *controls* to be the responsibility of accountants and auditors, and are not therefore prepared to accept ownership of them.

Managers, however, can see how *risks* directly affect them and are more likely to accept that it is their responsibility to manage them. In addition, since the internal controls necessary depend on the risks identified, a better definition of internal auditing involves risks. My own definition is:

Internal auditing provides an independent and objective opinion to an organisation's management as to whether its risks are being managed to acceptable levels.

Let's look at this definition in detail:

Independent: the function carrying out the internal auditing activity should be outside the normal management hierarchy, ideally responsible to a board executive, or similar, with a strong reporting line to the chairman of the audit committee. (My experience has shown that internal auditors are welcomed into departments since they don't have a 'political axe to grind'.) The Institute of Internal Auditors (U.K.) has issued a Professional Issues Bulletin on independence and objectivity (chapter 9 for a link).

Objective: objectivity is a state of mind; it doesn't depend on your boss. Opinions should be based on verifiable facts, viewed without bias.

Opinion: This is the keyword in the definition. The objective of the internal auditing is all about telling management, and through them the stakeholders, whether risks are being managed. The word 'assurance' is often used but it doesn't allow for the circumstances where assurance can't be given. An opinion can be good or bad.

Organisation: A group of people, with supporting assets, that are accountable to stakeholders. For example, external parties, such as shareholders, governments and trustees; or owners, such as partners and shareholders in a 'private' company. Such an organisation will normally have to prepare financial, and other, statements for these 'stakeholders'.

Management: The group of people accountable for these statements and for the proper operation of the organisation. I had thought of substituting 'stakeholders' for 'management', but the various rules (see chapter 2) are quite clear - management is responsible for making sure risks are managed, and reports go to this group. In public companies, 'management' is now being specified as the audit committee.

Managed: Risks are managed by using the response processes we have considered: terminate, transfer, tolerate, treat.

RBIA – Why does internal auditing exist?

Acceptable: This means that the response processes are managing risks to a level that management consider reasonable. This level is known as the 'risk appetite' of the organisation. Thus internal auditors have to understand this risk appetite, against which the significance of risks can then be measured. It also implies that, when management is assuring the board that it is controlling risks, the risk appetite must be understood by all. It is the board which defines the risk appetite, and which the internal audit activity must accept, even if it considers it is set too high or low. However, the board has a responsibility to its stakeholders and probably has to comply with legislation that requires it to maintain a proper system of internal control.

1.6 Where does 'risk management' fit in?

Now this is where the fun starts. What is risk management and what responsibility does the internal audit activity have? Let's start with some certainties:

- Managers own risks and it is their responsibility to control them.
- Internal auditing provides an opinion, to management, as to whether risks are properly controlled.

'Risk management' is a term widely used, and 'Risk Manager' jobs exist in organisations. Theoretically, since managers own risks, they must 'manage' them. That accountability cannot be passed to a third party. In practice, risk managers tend to have responsibilities between managers and the internal audit activity, assisting the organisation to identify its risks, running risk workshops, coaching staff in risk management and setting 'best practice standards'.

Internal audit activities may be asked to provide advice, and more, on risk management. An Institute of Internal Auditors (U.K.) publication (chapter 9) provides guidance as to how involved they should become.

Based on this, my advice to internal auditors would be to give as much assistance as you like provided:

- It doesn't compromise your independence and objectivity.
- The resources required don't hinder you from achieving your main objective of meeting your audit committee's targets .
- Managers don't come to regard you as the risk owner. You're providing an opinion to them, not the other way round.

My own experience has shown that, if risk managers exist, the responsibilities of internal audit and risk management must be clearly defined and communicated within the organisation. Ideally both functions should report to different senior managers or directors to reinforce the distinction.

Chapter 9 provides links to useful sites on risk management. I would also recommend the UK Treasury's 'Orange Book', which can be downloaded free.

1.7 Summary

So my current definitions may be summarised:

- **Risks** hinder **objectives**.
- **Internal controls** manage **risks**.
- **Internal auditing** provides opinions about whether **internal controls** are managing **risks** to acceptable levels.

RBIA – Why does internal auditing exist?

As you will see when you look at chapter 9 (Useful information) these are not standard definitions, although they do not contradict current thought. I prefer them because:

- They are simple
- They provide a clear trail from an organisation's objectives to all the internal controls it requires, and to the purpose of internal auditing. ([Appendix A](#) shows this relationship)

2 Does it have to exist?

2.1 Who says so?

Over the past few years there have been major company failures due to financial irregularities. This has inevitably led to several countries introducing regulations to tighten internal controls within companies. The primary regulations in the U.K. come from the London Stock Exchange Combined Code, backed up by the Turnbull Committee guidance. In the U.S., the Sarbanes-Oxley act is the legislation, supported by standards from the Public Company Accounting Oversight Board (PCAOB). See chapter 9 for their web addresses.

One area of business that is subject to special regulations is banking and finance. While risk based internal auditing is relevant to this area, it has additional requirements that I am not covering in this book.

2.2 London Stock Exchange

The London Stock Exchange (LSE) has published the 'Combined Code', which is appended to, but not part of, the LSE rules.

This was revised in July 2003, and incorporates two principles directly relevant to internal auditing:

Principle C2: The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets.

Principle C3: The board should establish formal and transparent arrangements for considering how they should apply the financial reporting and internal control principles and for maintaining an appropriate relationship with the company's auditors.

Both principles have further explanations under *Code provisions*. That for C2 is:

C.2.1: The board should, at least annually, conduct a review of the effectiveness of the group's system of internal controls and should report to shareholders that they have done so. The review should cover all material controls, including financial, operational and compliance controls and risk management systems.

There are 7 provisions for C3. Provision C3.2 outlines some of the responsibilities expected of an audit committee, which include:

- To review the company's internal financial controls and, unless expressly addressed by a separate board risk committee composed of independent directors, or by the board itself, to review the company's internal control and risk management systems.
- To monitor and review the effectiveness of the company's internal audit function.

Further guidance for C2 is provided by the Turnbull guidance and for C3 by the Smith guidance. More details on these are in the next sections.

Although the Combined Code is strictly relevant to UK listed companies, the principles and guidance notes are useful to any internal audit activity, and are worth reading. Links are in chapter 9. Its weak point is that it doesn't require the directors to report on the contents of the review of controls, only that a review has been carried out.

2.3 The Turnbull Guidance

When the Combined Code was originally published, the Institute of Chartered Accountants in England and Wales agreed with the Stock Exchange that it would provide guidance in implementing the code. The result was 'Internal Control: Guidance for Directors on the Combined Code', published by a working party chaired by Nigel Turnbull and therefore referred to as the 'Turnbull Guidance'. It is a relatively short (14 pages) document that should be read in full if you are a UK internal auditor. The Turnbull guidance was reviewed in 2005 and the important principles it sets down are:

- The board of directors is responsible for the company's system of internal control. It should set policies, and ensure internal controls manage risks (para. 15).
- It is the role of management to implement the board policies. It should identify and evaluate the risks faced by the company and design, operate and monitor a suitable system of internal control (para. 17 also para. 8).
- Reviewing the effectiveness of internal control is an essential part of the board's responsibilities (para. 24). (This applies to companies, but could equally apply to the trustees of a charity, or the governing body of a university).
- All employees have some responsibility for internal control as part of their accountability for achieving objectives (para. 18). (This supports my definitions, as it connects internal controls with objectives).
- The board should discharge its responsibilities by:
 - Receiving and reviewing reports on internal control (para. 26).
 - Undertaking an annual assessment on internal control.
- Internal controls should include all types of controls including those of an operational and compliance nature, as well as internal financial control (para. 12). (So my finding lorry drivers is OK then).
- Support for the board's statement should be appropriately documented (para. 26). (So write it down!).

I believe that the application of the Turnbull Guidance is universal, that is to all organisations and in every country. It clearly establishes the Board's responsibility for enterprise risk management (although it doesn't use that phrase), management's responsibility for managing risks and reporting on the effectiveness of controls to the board. Although it doesn't state the need for an internal audit department, the Smith guidance (below) effectively requires one. **It therefore clearly establishes the requirement, in UK quoted companies, for risk based internal auditing.**

The Financial Reporting Council website has full details of the Guidelines (see chapter 9).

2.4 The Smith Guidance

This guidance, like that of Turnbull, is also part of the Combined Code and provides advice on the role and responsibilities of audit committees.

The paragraphs relevant to internal auditing are 4.5 to 4.7 and 4.9 to 4.12:

4.5. The audit committee should review the company's internal financial controls (that is, the systems established to identify, assess, manage and monitor financial risks); and unless expressly addressed by a separate board risk committee comprised of independent directors or by the board itself, the company's internal control and risk management systems.

RBIA – Does internal auditing have to exist?

4.6. The company'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. Except where the board or a risk committee is expressly responsible for reviewing the effectiveness of the internal control and risk management systems, the audit committee should receive reports from management on the effectiveness of the systems they have established and the conclusions of any testing carried out by internal and external auditors.

4.7. Except to the extent that this is expressly dealt with by the board or risk committee, the audit committee should review and approve the statements included in the annual report in relation to internal control and the management of risk.

These paragraphs allow an unscrupulous board to restrict to responsibility of an independent board committee to financial controls only. Since the audit committee oversees the work of the internal audit activity, its responsibilities could similarly be restricted, preventing it from considering all significant risks to the company. I still believe the audit committee should review all the company's internal controls, with no opportunity for other committees to take responsibility for the non-financial risks.

Paragraph 4.9 requires the audit committee 'to monitor and review the effectiveness of the company's internal control function'. Paras. 4.10 to 4.12 provide advice as to how 'effectiveness' might be judged, which includes adherence to the IIA standards (see 4.10). Paragraph 4.12 also notes requires the audit committee to 'monitor and assess the role and effectiveness of the internal audit function in the overall context of the company's risk management system'. Another clear link between risks and internal audit.

One further responsibility, especially bearing in mind the requirement in the US for external auditors to report on the 'effectiveness of the internal control structure', (Sabanee-Oxley Act below), is 4.35: 'Obtain feedback about the conduct of the [external] audit from key people involved, e.g. the finance director and the head of internal audit'.

Internal auditing is beginning to gain its rightful place!

2.5 Sarbanes-Oxley

This is a U.S. act, much of it being devoted to the setting up of a Public Company Accounting Oversight Board (PCAOB) and its responsibilities. The main impact of the act for internal auditors is contained in S302 and S404. S404 states:

- Companies are required to state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting
- Management is required to prepare a report annually on the effectiveness of the company's system of internal control as it relates to financial reporting.
- The company's external auditor must report on the reliability of management's assessment of internal control.
- The internal control report must:
 - State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.
 - Contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
- With respect to the internal control assessment required by this section, each registered public accounting firm that prepares or issues the audit report for a company shall attest to and report on, the assessment made by the management of that company.

Sections 103(a)(2)(A) and 404(b) of the Act direct the PCAOB to establish professional standards governing the independent auditor's attestation and reporting on management's assessment of the effectiveness of internal control over financial reporting.

It seems to me, after a rather superficial look at the act, that it concerns management and external auditors only and that the internal audit activity is unaffected, as far as its responsibility for *internal auditing* is concerned. After all, the IIA hasn't changed its definition of internal auditing as a result of 'SOx'. If only life were so simple. Because the internal audit activity are the experts on financial controls they have been recruited to carry out much of the documentation and other tasks required by SOx, thus reducing the time available to address the really big risks.

Unlike the Turnbull Guidance, SOx doesn't set down wide-ranging principles but introduces tougher regulations for financial reporting. I have a suspicion however that more money is lost by companies and their shareholders through the bad decisions of boards (that is, their failure to manage risks) than through inaccurate financial accounts.

2.6 PCAOB standards

The PCAOB issued Auditing Standard No. 2 on March 9, 2004. Its subject is, 'An audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements'. It's a long title for a long document (211 pages – link in chapter 9).

The standards are intended for external auditors and internal audit features mainly in the section: 'Using the work of others' (paragraphs 108 to 126). Paragraph 128 notes the need for the external auditor to review reports issued by internal audit, where they relate to financial controls. If an internal audit function is ineffective a significant deficiency could result (paragraph 140).

RBIA – Does internal auditing have to exist?

The 'Key Provisions', section 7 notes; "This considerable flexibility in using the work of others should translate into a strong encouragement for companies to develop high-quality internal audit, compliance, and other such functions. The more highly competent and objective these functions are, and the more thorough their testing, the more the auditor will be able to use their work."

The standards seem to expect external (independent) auditors to report on the reliability of management's assessment by carrying out in-depth testing.

I'm unclear on the role of the internal audit activity. It could be used

- To assist management in their assessment of the effectiveness of internal controls over financial reporting
- To report on management's assessment, and hope that this will reduce the work the independent auditor has to do, and therefore charge for.

In either case, the work of the internal auditor will have to be to the same, or higher, standard as the independent auditors, in order to reduce their work to the minimum. It will also have to follow the IIA Professional Practices Framework.

But what about risk based internal auditing? Many risks which threaten the objectives of companies are far greater than even material financial reporting risks. For example, loss of a warehouse as a result of fire could put a company out of business far quicker than an incorrect stock calculation, even if material. The risk based internal auditor will need to include the risks of material errors in financial reports alongside other risks and agree with the audit committee the priority of work.

I'm still unhappy with the fundamental concept which requires that management and the 'independent' auditors carry out more work to comply with more standards, when they couldn't comply with the previous standards. Yet the internal audit activity, which is the only group of people to come out of recent financial scandals with any credibility, are still not given sufficient prominence. I would like to see internal auditors given the right to audit the work of the 'independent' auditors and report their conclusions to the audit committee and PCAOB. The irony is that the standard does require the external auditor to give an opinion on the internal financial controls, which is not required by the London Stock Exchange's Combined Code which, in other respects I consider is the better standard.

2.7 Institute of Internal Auditors

The Institute's 'Professional Practices Framework' consists of: a Code of Ethics and standards; practice advisories; development and practice aids. Details of their site are available in chapter 9.

Their definition of internal auditing (included in the Code of Ethics) is:

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

I don't like this definition for several reasons:

- The first sentence places too much emphasis on 'consulting'. If management consider a primary objective of internal auditing to be consultancy there is the danger that, if management consider they don't need consultants, they also decide they don't need internal auditors!

RBIA – Does internal auditing have to exist?

- The most important part of internal auditing, assurance, is not designed primarily to add value by improving an organisation's operations, but to assure the management that these operations do not have unacceptable levels of risk, and report where they do. For example, if consultants have just looked at the operations of our accounts payable department, we can assume it's efficient and we cannot add further value. The definition above would imply we don't then need to audit it, yet we should audit it to provide assurance that the consultants haven't removed important controls! In this instance the IIA definition could lead us to the wrong decision.

So how do we justify our existence if our primary aim is not to add value? Well, we *preserve* value - and we provide the executive with a 'Get out of jail free' card.

- The definition doesn't indicate who is assured by internal auditing.
- The second sentence could be applied to any part of the organisation, since risk management is a line management responsibility.

I think I'll stick with my definition, until one which I like better comes along.

The U.K. IIA has published a guidance note, *An approach to implementing Risk Based Internal Auditing*. See chapter 9 for the link.

The IIA standards do mention risks:

Performance Standard 2010 - Planning - The chief audit executive should establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals.

Implementation Standard 2010.A1 (Assurance Engagements) - The internal audit activity's plan of engagements should be based on a risk assessment, undertaken at least annually. The input of senior management and the board should be considered in this process.

Implementation Standard 2010.C1 (Consulting Engagements) - The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Those engagements that have been accepted should be included in the plan.

Performance Standard 2200 - Engagement Planning - Internal auditors should develop and record a plan for each engagement, including the scope, objectives, timing and resource allocations.

Performance Standard 2201 - Planning Considerations - In planning the engagement, internal auditors should consider:

- The objectives of the activity being reviewed and the means by which the activity controls its performance.
- The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.
- The adequacy and effectiveness of the activity's risk management and control systems compared to a relevant control framework or model.
- The opportunities for making significant improvements to the activity's risk management and control systems.

There doesn't seem to be much further guidance from the IIA in the US as to how to implement an auditing methodology centred on risks. Perhaps that's why many auditors still rely on audit programmes.

2.8 Management

Does internal auditing have to exist for management? What do they want from the process? In 2003 Deloitte & Touche and the Institute of Internal Auditors – UK and Ireland (IIA) carried out a survey to answer this question. The main conclusion was:

“Both board directors and heads of internal audit agree that the biggest ways that internal audit adds value are providing assurance that the main business risks are being managed and providing assurance that the general internal control framework is operating efficiently” (Chapter 9 for details).

2.9 Summary

Does internal auditing have to exist? In the UK, for listed companies, national government departments, local government and the National Health Service the answer is ‘yes’. In all cases it is required to report on the effectiveness of internal controls in managing the organisation’s risks.

Risk based internal auditing is the methodology which delivers that requirement. The rest of this introduction shows one way in which the methodology can be put into practice.

3 How does internal auditing find the risks?

3.1 *The role of internal audit*

We've learnt that:

Internal auditing provides an independent and objective opinion to an organisation's management as to whether its risks are being managed to acceptable levels.

Which can also serve as the definition of risk based internal auditing!

It is management's responsibility to identify, assess and manage risks, so where does the internal audit activity fit in? It doesn't, since it's management's responsibility to pass over a list of risks to us, on which we can then base a plan of work (an audit plan) to deliver the internal auditing objective above.

In the real world life isn't so simple...

3.2 *The role of management*

In some organisations management will set up a framework to identify, assess and manage risks, possibly appointing 'risk mangers' to do this. In other organisations, the internal audit activity will be asked to help, and in the remainder not much will happen at all. Guidance on the extent of the internal audit activities help is provided in the IIA publication *The role of Internal Audit in Enterprise-wide risk management*.

The complete identification of risks, by management, is the most important part of risk-based internal auditing, as well as being vital to the proper operation of any organisation.

We'll assume that the internal audit activity is helping to identify and evaluate risks. Since it is to use the risks identified, this has its advantages.

So how are we to help management in determining the organisation's risks?

Well, we could rush off and collect risks from everyone, but there are two problems:

1. How do we know this will collect *all* the significant risks?
2. How do we drive out an audit plan from these risks?

So let's stop and think. Before we start, why not try to anticipate what we would expect to find as risks, and work through the process to an audit plan. Thinking through the process beforehand will help us to focus our questions when we start meeting people.

3.3 *Finding and evaluating all the risks*

3.3.1 Finding risks and controls - an example

Let's take an example – a charity with the **objective**: 'Relieve famine in central Africa'. (I've chosen a charity as an example, in order to illustrate that we can use the risk based audit approach for any organisation. I should state that I have no experience of this type of charity!)

The significant 'top level' **risks** might be

1. No clear strategy as to how to achieve our objective.
2. Unable to predict where and when famines will occur.
3. Unable to obtain food.

RBIA – How does internal auditing find the risks?

4. Unable to deliver the food to the starving.
5. Do not have the staff and systems to support the operation.

What **internal control** processes might we expect to manage these risks?

1. Written strategy approved by the trustees.
2. Reports from people in Africa.
3. Establish links with food aid providers.
4. Establish a supply chain involving ships and lorries.
5. Office staff supported by finance and communication systems.

These risks and controls can be arranged in a hierarchy ([appendix B](#)).

Nothing difficult so far – but we can't really drive manageable audits out of these risks. For example, an audit of the supply chain might involve everything from paying for shipping grain, through making sure we had spare parts for our lorries, to checking that bridges along the route would take the weight of these lorries.

3.3.2 Objectives and processes

So we need to break down the risks further. How? We've seen that risks hinder objectives but an organisation's objectives are delivered by *processes*, which may be a straightforward task, such as loading goods on a lorry, or may be a reaction to a risk, such as employing mechanics to stop lorries breaking down. The distinction is not always clear, or important, at this stage.

It is sometimes easier to look at the risks which threaten processes which deliver the objectives, rather than the objectives themselves. So, for example, let's take the supply chain process (4) and look at the risks which might hinder it.

Process: Establish a supply chain involving ships and lorries

Risks:

1. Unable to obtain space on ships.
2. Insufficient lorries to transport grain.
3. Lorries break down.
4. Insufficient drivers.
5. Roads are impassable.
6. Do not know where food is required most urgently.

Internal controls:

1. Determine shipping lines which serve the ports nearest to central Africa.
2. Buy lorries and/or identify other sources for lorries.
3. Maintain lorries, employ mechanics.
4. Employ drivers.
5. Identify all possible roads and identify those which are suitable, and when.
6. Set up a system for receiving reports from food distribution points.

RBIA – How does internal auditing find the risks?

We could carry on, as these control processes are hindered by risks and could be further subdivided. So we have established a hierarchy, of which appendix B is a part.

This method of looking at risks which hinder those processes which deliver objectives has the advantage of establishing a structure for the risks, which makes it easier for management to ensure the risks identified are complete and easier to structure the audit work necessary to check the management of those risks. However:

- The underlying objectives of the organisation must not be forgotten
- The processes documented are those used to deliver these objectives NOT the actual processes the organisation actually uses. There should be close agreement, but the organisation may not be operating some processes necessary (such as internal controls) or may be operating some processes which are not necessary.
- Where risks are not being managed to acceptable levels, the underlying objective, which may not be achieved, should be identified (more later).

3.3.3 The process map

However:

- There are many levels in the hierarchy, making it complicated.
- We are now in a position to identify audit topics and don't need to go further - at this stage. For example, one audit could provide assurance on the provision of lorries and drivers to transport grain. (A single audit can provide an opinion as to whether several risks are managed to an acceptable level.).

So how do we simplify the whole structure? Well by taking:

- The risk threatening a higher level process
- The internal control process which manages it

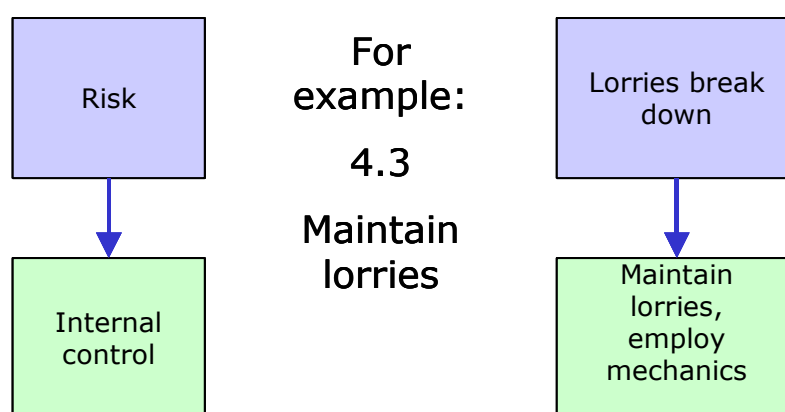


Fig. 1 Composition of a process

and summarising these as a **process**.

We can now simplify the hierarchy (appendix B) into a **Process Map** – see [appendix C](#). (It is useful to number each process as shown). The process map takes the organisation's primary objective and identifies the processes necessary to deliver it, in ever increasing detail down to a level at which we wish to plan individual audits.

RBIA – How does internal auditing find the risks?

The advantages of a process map are:

- It will incorporate all the logical processes required to achieve the organisation's objectives, after it has been agreed by management.
- It is independent of the departments and people in the organisation, and so, when they change, we don't have to change the map, only the owners of the processes.
- It is relatively easy to identify all the necessary processes required to achieve the organisation's objectives. By linking risks to these processes we can therefore be reasonably sure that we have identified nearly all the significant risks.
- We can compare our 'logical' processes to those actually in use to see if any are missing, or are not required.
- By scoring (see later) the risks relating to each process, we can identify the processes hindered by the most significant risks and audit these first.
- We can define audits in terms of the processes included in that audit. Thus enabling us to easily identify our audit coverage.

Because we are talking about processes, it is vital at this point that we distinguish between risk based internal auditing and systems (or processed) based auditing.

- Risk based internal auditing is driven by risks and reports whether these are being managed. Processes are only used to help categorise a large number of risks, and these processes should be 'logical' and not actual. If you have a risk but can't allocate to a process, then think up a new process!
- Systems based internal auditing is driven by the actual systems in place and controls are related to these. It assumes that the systems in place cover all risks and frequently relies on 'internal control questionnaires', that is standard documents used every time an audit is carried out. The danger of using these programmes is set out in 7.8.2.

So we have now got a logical structure for our organisation, which will be used to help management identify *all* significant risks. We now need a means of deciding the significance of each risk, so:

- Management can decide how to manage them.
- We can target audits at those posing the greatest threat.

RBIA – How does internal auditing find the risks?

3.3.4 The elements

There are two elements of a risk:

- The Consequence (also called impact) when a risk occurs.
- The Likelihood (also called probability) of the risk occurring.

The measure applied to each can be complex, but the following is relatively simple. There are five levels applied to each element, defined as below:

If the consequence when the risk occurs is:	OR the likelihood of the risk occurring is:	Then the measure is defined to be:
To close down the organisation, or a significant part, for a very long period	Almost certain	Very high (5)
To prevent the organisation achieving a major part of its objectives for a long time	Probable	High (4)
To stop the organisation achieving its some of its objectives for a limited period	Possible	Medium (3)
To cause inconvenience but not affecting the achievement of significant objectives	Unlikely	Low (2)
To cause very minor inconvenience, not affecting the achievement of objectives	Rare	Very Low (1)

If possible, it is useful to put values to the consequence score, for example, a cash loss over £1m might be considered very high if it threatened the existence of the organisation. However, don't get carried away with a need for accuracy, remember we only need an approximate value to determine where we audit.

Since we need to sort risks, it helps to attach numbers to the risk measure (for example 4 for 'High'). Consequence and likelihood can be multiplied together to give a single measure of the significance of a risk, or a different combination can be used. For example, take the risk that a lorry may break down. Assuming we have only three, old lorries, the consequence could be medium (scores 3) but the likelihood could be high (scores 4), giving a significance of 12.

3.3.5 Before or after internal controls?

Risks are ideally scored before and after taking account of the response which manages the risk.

- **Inherent** (or **gross** or **absolute**) risk scores are measured by assessing the consequence and likelihood of a risk occurring before any internal controls are taken into account.
- **Residual** (or **net** or **controlled**) risk scores are measured by assessing the consequence and likelihood of a risk occurring after any internal controls are taken into account.

RBIA – How does internal auditing find the risks?

In practice, it is relatively easy to measure inherent risks for new projects, since there are no controls yet in place. However, for ongoing operations it is much more difficult. Measuring the consequences is not too difficult, since most controls don't reduce these, but only the likelihood. But what's the likelihood of a risk occurring if we have no controls – almost certain every time! It's for this reason that, when carrying out interviews, or a risk workshop, the best risks to measure are residual risk, since people naturally assume controls to be in place.

The main danger, of course, is that there is an assumption that controls are present and operating. Since it is the purpose of internal auditing to provide an opinion to management as to whether these controls properly manage risks, the internal audit plan should be chosen on the basis of inherent risk, not residual risk. So, there is no real reason to determine the mitigating controls, and score the residual risk, since this will be done as part of the audit. In practice it is better to do this because:

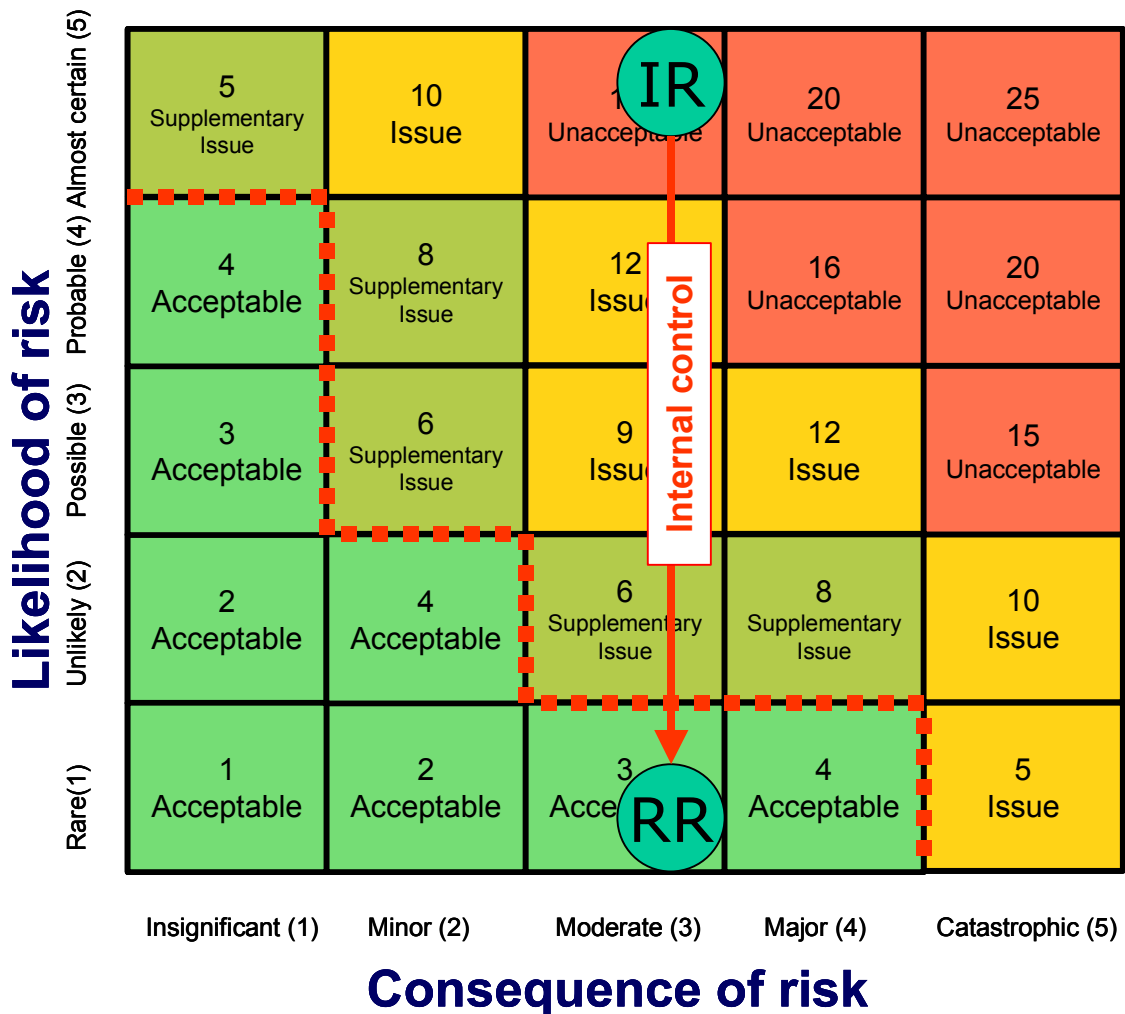
- The residual risk is the only measure we may have from risk workshops.
- It checks our scoring of the inherent risks. For example, a residual risk with an consequence of high (4) cannot have an inherent score with a consequence of medium (3) unless the internal control had actually increased the risk!
- The audits which may need high priority are those with a high residual risk – since we know we have got problems in these processes.

3.4 What risks are we prepared to accept?

We have talked about managing all risks to acceptable levels. Now we have scored risks before and after internal controls we can begin to define the organisation's 'risk appetite'.

One method of deciding which risks to accept is to place them on a grid of likelihood and consequence (see below). This enables the board to define the action it requires management to take for each likelihood/consequence combination. The boundary between the acceptable risks and those which require managing is known as the 'risk appetite'. If inherent risks cannot be managed below this line by 'treatment' then they will have to be terminated, transferred or tolerated.

RBIA – How does internal auditing find the risks?



- 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

Note that the board have determined that a risk with catastrophic consequences and rare likelihood requires action to manage it, even if it only has a score of five. Of course that action may be to 'tolerate' the risk if it cannot be cost-effectively reduced.

The risk appetite could be set higher for different parts of the organisation, or for development projects aimed at increasing the value of the organisation.

The diagram also shows the potential impact of internal controls in reducing an unacceptable risk to an acceptable risk. **Risk-based internal auditing is all about providing an opinion as to whether these controls are managing risks to an acceptable level.**

RBIA – How does internal auditing find the risks?

So now we can assign risks to a structure, measure them and assess their significance' let's get out and find out what people think are the real, significant risks.

3.5 Finding the significant risks

3.5.1 Start at the top

Who knows the significant risks – the most significant people. That is, the board of a company, the partners, the trustees of a charity or the Vice-chancellor and senate of a university.

So you really have to start with them. How? Well the Institute of Chartered Accountants in England and Wales has a useful booklet 'Implementing Turnbull – a boardroom briefing' (chapter 9 for the link). I can't add much to this document except some practical advice (below) from colleagues who have worked with executives in determining risks.

There are three basic methods of determining risks:

- Interviewing
- Risk workshops
- The accounts

If your organisation has a 'Risk Management' function, it is they who will probably be involved in using these techniques.

3.5.2 Interviewing

The output from an interview is an individual's view of the risks hindering the organisation's objectives. The advantages of an interview are:

- It's easier to arrange than trying to get a group of people together.
- People may be prepared to express their concerns, which they may not wish to do in a meeting. This should give rise to a wider range of risks than from a meeting.

The disadvantages are:

- The wide range of risks will be more difficult to categorise.
- You will still have to run a risk workshop to get consensus on the consequence and likelihood of risks.

Some practical tips for interviews are given in [appendix D](#).

3.5.3 Risk workshops

The output from a risk workshop is a list of risks, which could hinder the processes or project being considered, with a measure of their consequence and likelihood.

Risk workshops can be used:

- with the most senior people in an organisation, to get the significant risks.
- with members of a project team, to highlight the risks facing the project.
- with people involved in an audit, to highlight any issues already known.

The advantage of a risk workshop, over interviews of individuals, is that people interact with each other to produce new ideas. Risks workshops are useful at the start of audits because they help get 'buy-in' from the departments involved.

RBIA – How does internal auditing find the risks?

Details of how a risk workshop can be run are included in [appendix E](#).

3.5.4 The accounts

We should examine the accounts of the organisation, both the figures and the surrounding processes with the management concerned.

For each of the headings in the accounts, what represents the significant risks? For example, in banks these might include the 'bad debts provision', but for retailers these might include the 'obsolete stock provision'. Don't only look at figures that might be unusually high, but those which are unusually low. We might expect these figures to be checked by the external auditors but the failure of WorldCom, and others, shows this trust might be misplaced.

3.6 Recording the risks

3.6.1 What we've got so far

- A list of risks which are considered significant by the people that own them - management. Some may have been prioritised in risk workshops.
- A process map, updated from interviews and risk workshops. For example process 5.1 (Raise money) on our original process map ([appendix C](#)) has been raised to 5 (Acquire funding) to indicate its importance. (I've not included an updated appendix C but the risk register, discussed later, shows the amended structure).

It will have taken some time, and considerable effort to reach this stage. While some people will understand the purpose of identifying risk, others will consider it a waste of time. Getting management to support and contribute to the identification of risks is one of the most difficult parts of risk-based internal auditing. In addition, our list of risks will be broad and some may look as if they will never match up to our process map.

In particular:

- Many risks will focus on new projects which don't have any processes. These effectively link up to process 1.3 (Delivery of strategy) but when it comes to audit planning each project will have to be evaluated to assess its risk.
- Some risks will be very broad covering most, if not all processes. Such risks include:
 - the ability to recruit good staff.
 - the lack of contingency plans.
 - fraud.

In practice these are included as additional processes under 'Support' (5 in appendix C) but considered for inclusion in all audits. Appendix L gives some ideas.

We might be tempted at this stage, faced with a pile of risks not easily linked to processes, to do a quick evaluation to determine the most significant risks, base an audit plan on these and go and find if there are sufficient controls to manage them. However this approach has problems:

- We don't know if the organisation has captured all its risks, and we have a record of them. While we are unlikely to have the specialist knowledge to ensure all risks have been captured, linking those which have been identified to a process map will help us spot obvious gaps.

RBIA – How does internal auditing find the risks?

- We may plan audits which cover the same processes several times.
- The lack of structure in a list of risks will make it difficult to talk about the audit plan, and its achievements, to the Audit Committee and other interested people.

So, we need to allocate the risks which have been identified, to those processes hindered by them. We then determine the most significant risks, and build the audit plan to check if these are adequately managed by internal controls.

3.6.2 The risk register

Since risks will have to be scored and sorted, they are best input into a 'database'. This can be held in a spreadsheet (for example 'Excel'), or database program (for example 'Access'). We start by putting the process map into the database, adding risks and scoring them. [Appendix F](#) shows part of this database, held on a spreadsheet, which is known as the *risk register*. Since each risk is to be scored and sorted, the processes to which it is attached are repeated in the appropriate columns. (To view the whole database, download the spreadsheet from www.internalaudit.biz.) If some risks affect more than one process, they will have to be repeated. (The advantage of using a proper database is that one risk can be linked to several processes, as well as several risks to one process. Chapter 9 has links to web sites of software suppliers.)

As we saw when drawing up the process map, since the aim of the register is to set up an audit plan, we only have to break down the processes to a level low enough to identify audits. Hence many processes are only broken down to level 2.

I should also add that the register would be built up over many weeks and be much more comprehensive than Appendix F. Take it as an illustration, not 'best practice'!

We could now add those controls we have been told are present and score the residual risks. (I haven't done this). It isn't essential, as we will have to verify the proper operation of the controls as part of our audit work.

3.6.3 Updating the register

Since management is accountable for the control of risks, the register is effectively owned by *the managers*. They should agree to its content and scoring. They should be involved in regularly updating it with new risks, removing those no longer in existence and re-scoring risks, where necessary.

3.7 Life in the real world

3.7.1 Levels of risk maturity

In the real world we may not get the opportunity to influence the compilation of the risk register. If we are lucky, it may be collection of risks put together by managers who have been properly trained. If we are unlucky we may get a collection of risks thrown together by untrained managers who want to get on with their 'real' jobs. The degree to which the organisation understands risks and has implemented risk management is known as its *risk maturity*.

The IIA – UK and Ireland publication on 'Risk Based Internal Auditing' (link in chapter 9) defines five levels of risk maturity: risk enabled, risk managed, risk defined, risk aware and risk naïve. Since the effectiveness of RBIA revolves around a reliable risk register, we need to understand the characteristics of each type, and then decide where our organisation fits!

RBIA – How does internal auditing find the risks?

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 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. 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 from the internal activity will be necessary, since management will know the action to be taken.

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

Similar to the risk enabled approach. 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. The internal audit activity 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, we will have to facilitate the identification of risks, using workshops and interviews. 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. We will act as a consultant to undertake a risk assessment (in conjunction with management) to determine the work required to implement a risk framework that 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.

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

3.7.2 The impact of risk maturity

If our organisation is only risk aware or risk naïve, there are some unpleasant consequences:

- 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 we should report this to the audit committee.
- If our organisation has this level of risk maturity, we don't have a reliable risk register and, I would argue, we cannot therefore implement RBIA. Some would disagree, believing it is possible to use RBIA, based on the internal audit activity's own analysis of risks. This is a very dangerous approach, not only are internal auditors unlikely to be able to produce the comprehensive risk register necessary but it only encourages management to continue believing that internal auditors own the risks!
- Risk driven individual audits are possible. These rely on risks being determined as part of the audit work and require management training and risk workshops to determine risks in the areas being audited. The internal audit activity 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.

4 RBIA – the foundations

4.1 What is risk based internal auditing?

I don't think risk based internal auditing is different from internal auditing. Or, in other words, internal auditing is the same as risk based internal auditing and should use the RBIA methodology.

This is a very controversial statement, as it implies that all the other methodologies used by internal audit activities should be replaced - and that includes all those standard audit programmes. There is more on this argument in the section on the impact of RBIA.

Let's return to the definition of internal auditing:

Internal auditing provides an independent and objective opinion to an organisation's management as to whether its risks are being managed to acceptable levels.

4.2 The organisation's requirements

The definition of RBIA requires that the organisation:

- Knows all its significant inherent risks, that is, all those above its risk appetite.
- Has evaluated these risks so that they can be prioritised in order of the threat they represent.
- Has defined its risk appetite such that inherent and residual risks can be evaluated to determine whether they are above or below it.

These requirements imply:

- That the board has set appropriate policies on internal control.
- That the board has approved the risk appetite.
- That the management has been properly trained to identify and evaluate risks, and to design, operate and monitor the system of internal control which implements the policies adopted by the board.

If we haven't been involved in the process of compiling the risk register, one of our first jobs is to audit it for completeness and accuracy.

4.3 The RBIA stages

RBIA is all about providing an opinion on whether risks are being properly managed. So the work we have to do is:

1. Confirm the organisation's *risk register* is suitable for us to use as a basis for planning.
2. Decide those risks on whose management we are to provide an opinion and when. Group these risks into audits, that is compile the *risk and audit universe*. Compile an *audit plan*, probably annual, for approval by the audit committee.
3. Carry out the *individual audits* that will provide the opinions. Deliver a periodic (at least annual) *report* to the audit committee, and update the risk and audit universe as necessary

RBIA – the foundations

In practice, stage 1 will need to be done only once, or until we are confident in the risk register! The universe will need to be regularly updated as risks change and audits are completed. Stage 2 will be done annually, although the plan will probably change throughout the year.

We will consider stage 1 in this chapter, 2 in chapter 5, and 3 in chapter 6.

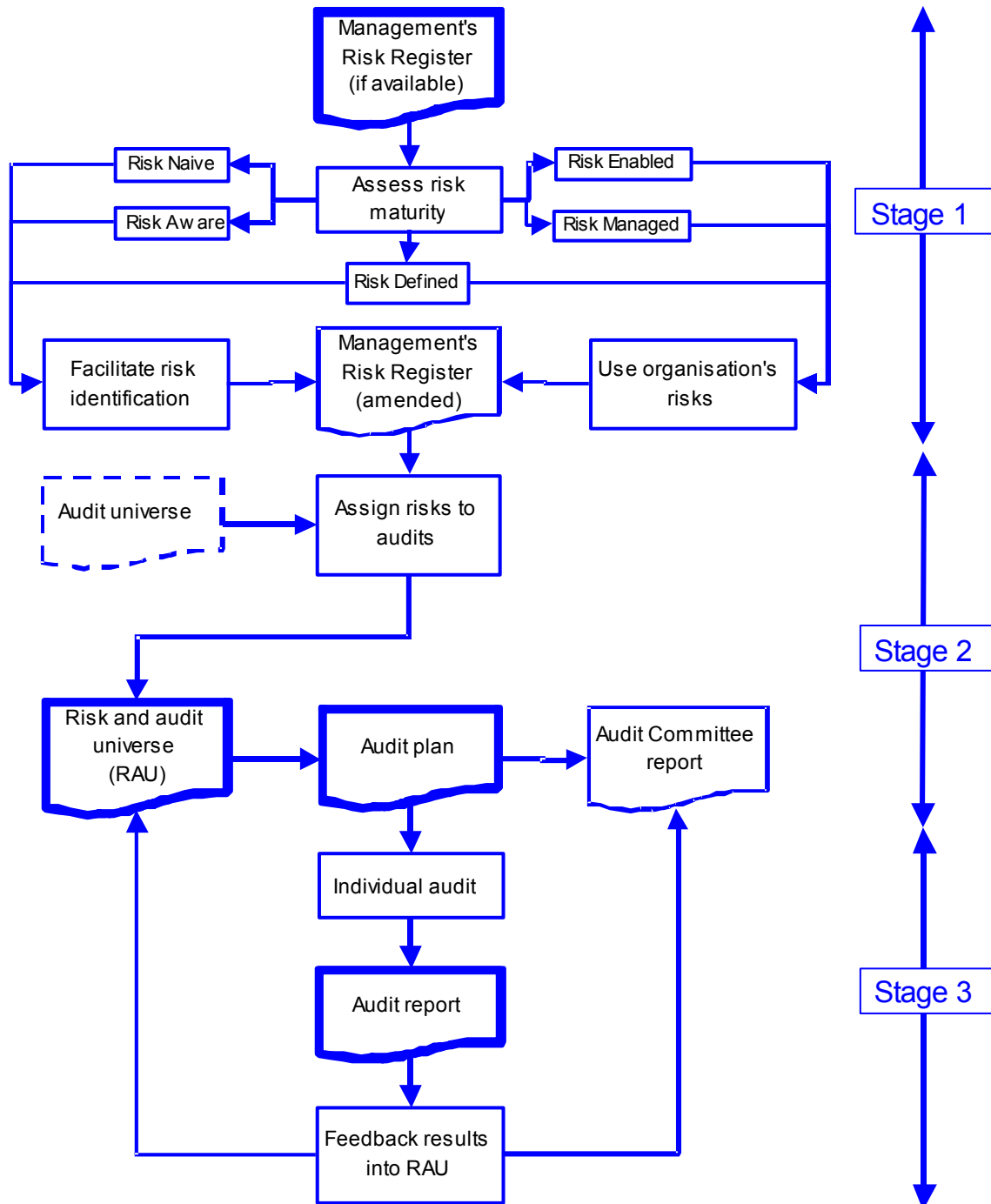


Fig 3 Stages of an audit

4.4 The RBIA Documentation

We'll deal with the detail later on, but it's useful to consider the overall methodology at this point. There are two documents which drive the methodology detailed in this book:

4.4.1 The risk and audit universe (RAU)

This is an extension of management's risk register and is best kept as a database, either on a spreadsheet (for example Excel), a database (for example Access) or a database especially for the purpose (see chapter 9 for suppliers). The RAU contains

- The risks that management has identified, and their score.
- The processes, and possibly objectives, that the risks threaten.
- The owner of the risk.
- The audit that provides an opinion on the management of each risk.
- Details of the last and next audits.
- Details of controls managing the risk.

Since a database can be sorted, it is possible to produce reports showing:

- Audits in the current audit plan
- Risks, in order of the processes they threaten. This assumes processes are uniquely numbered as has been done in the examples in this book
- Risks, in order of their significance, using the inherent risk score.
- Many other reports, including those showing resources, depending on the data held.

For an example, see appendix H in the spreadsheet downloadable from www.internalaudit.biz

4.4.2 The audit database

It would be theoretically possible to include all the organisation's risks in the RAU but this would usually result in a huge database that is difficult to manage. One of the advantages of using special software is that it is capable of recording all the risks.

The solution to this problem is to set up a separate database for each audit. This is similar in layout to the RAU but shows more detailed processes and audit tests and results. It links in with the RAU by incorporating the high level processes and risks that are relevant to the audit. There is therefore an 'audit trail' from the audit to the RAU. For an example, see appendix K in the spreadsheet downloadable from www.internalaudit.biz.

Since this database holds most of the information relevant to an audit, it replaces much of the documentation necessary and links in with the audit report.

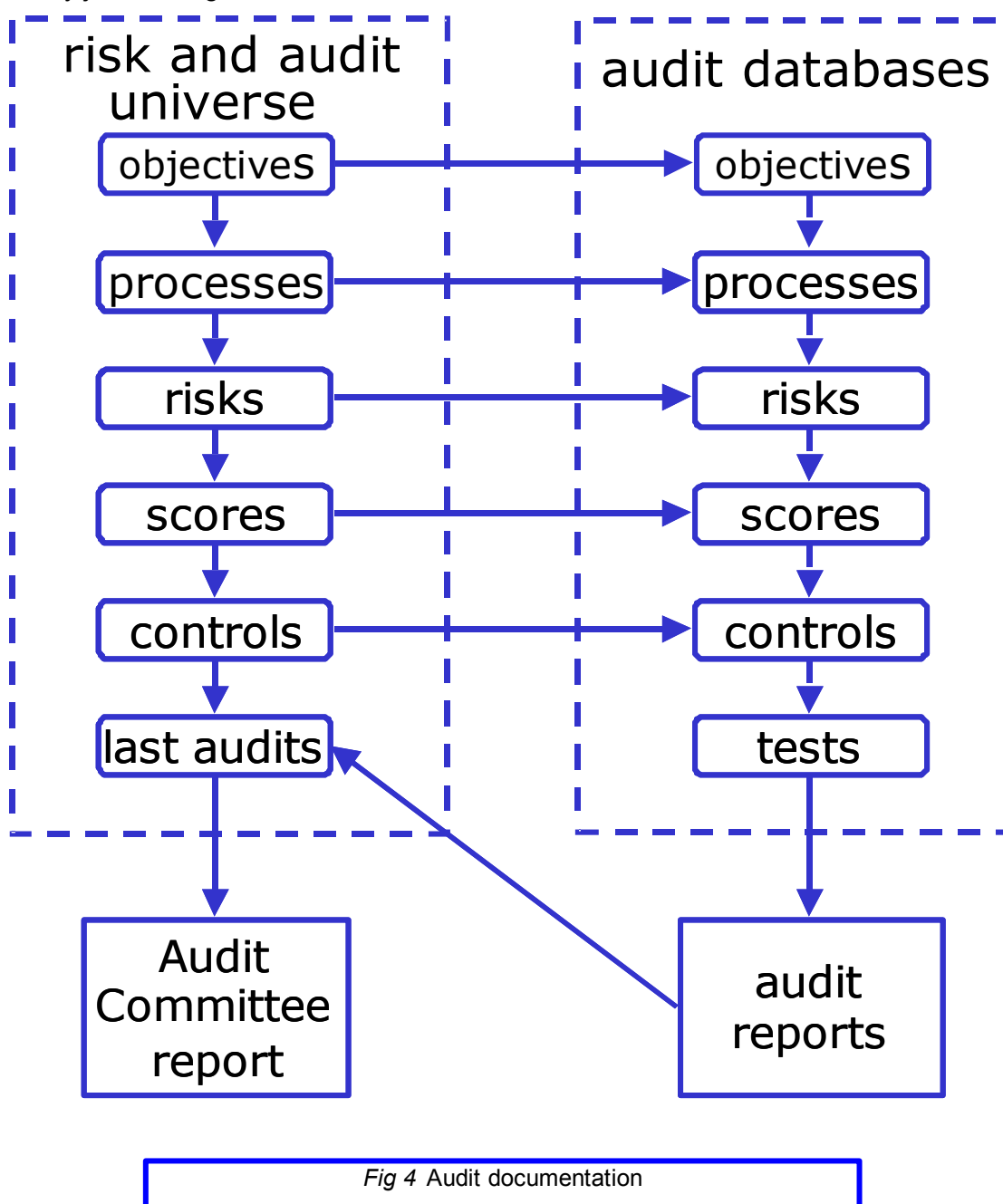
4.4.3 Other important documentation

The *Report to the audit committee* summarises the results from the individual audits and is derived from the RAU.

The *Audit Report* presents the results of an individual audit and is derived from the audit database.

4.4.4 Summary

The diagram below summarises the important documentation and shows the 'audit trail' that RBIA provides. It makes it possible to see how any individual test relates to the overall opinion provided to the audit committee and allows this opinion to be easily justified, right down to individual tests.



4.5 Stage 1 - Reliability of the risk register

4.5.1 Objective of the stage

We now need to demonstrate that risks above the risk appetite have been identified and correctly evaluated by management in order to assess whether the risk register can be used as the basis for the RAU and audit planning.

4.5.2 Internal audit work

- **Discuss the understanding of risk with the board and senior managers.** Determine what has already been done to improve the risk maturity of the organisation such as training, risk workshops, questionnaires about risks and interviews with risk managers.
- Ask for documents which detail:
 - The objectives of our organisation.
 - The methods to be used by managers to determine the significant risks that threaten the processes for which they are responsible.
 - The scoring system to be used for assessing the significance of risks. Ideally this will include values for a 'consequence' scale.
 - The board's statement of risk appetite.
 - How a consideration of risk is to be embedded into management's decision processes, particularly project management.
 - Our organisation's risks, preferably structured in some way which enables an opinion to be made as to how complete they are (the risk register).
- Examine the documents, check that procedures are adequate and have been followed, throughout the organisation.
- The IIA-UK and Ireland Guidance *An approach to implementing Risk Based Internal Auditing* has a very useful appendix A which shows criteria and tests to assess the level of risk maturity.

4.5.3 Opinion

Reach a conclusion as to the suitability of the risk register as a basis for audit plans.

- If it can be used, with minor improvements if required, ask management to make these.
- If it cannot be used for all, or parts of, the organisation, we decide on whether we are willing to facilitate improvements. We report to the audit committee that there is no complete list of evaluated risks and discuss other strategies for selecting areas to audit.

4.6 Stage 2 - Compiling the risk and audit universe and audit plan

4.6.1 Objective of the stage

- To decide which risks should be included in the audit plan
- To allocate risks to the audits that will provide an opinion on their management.

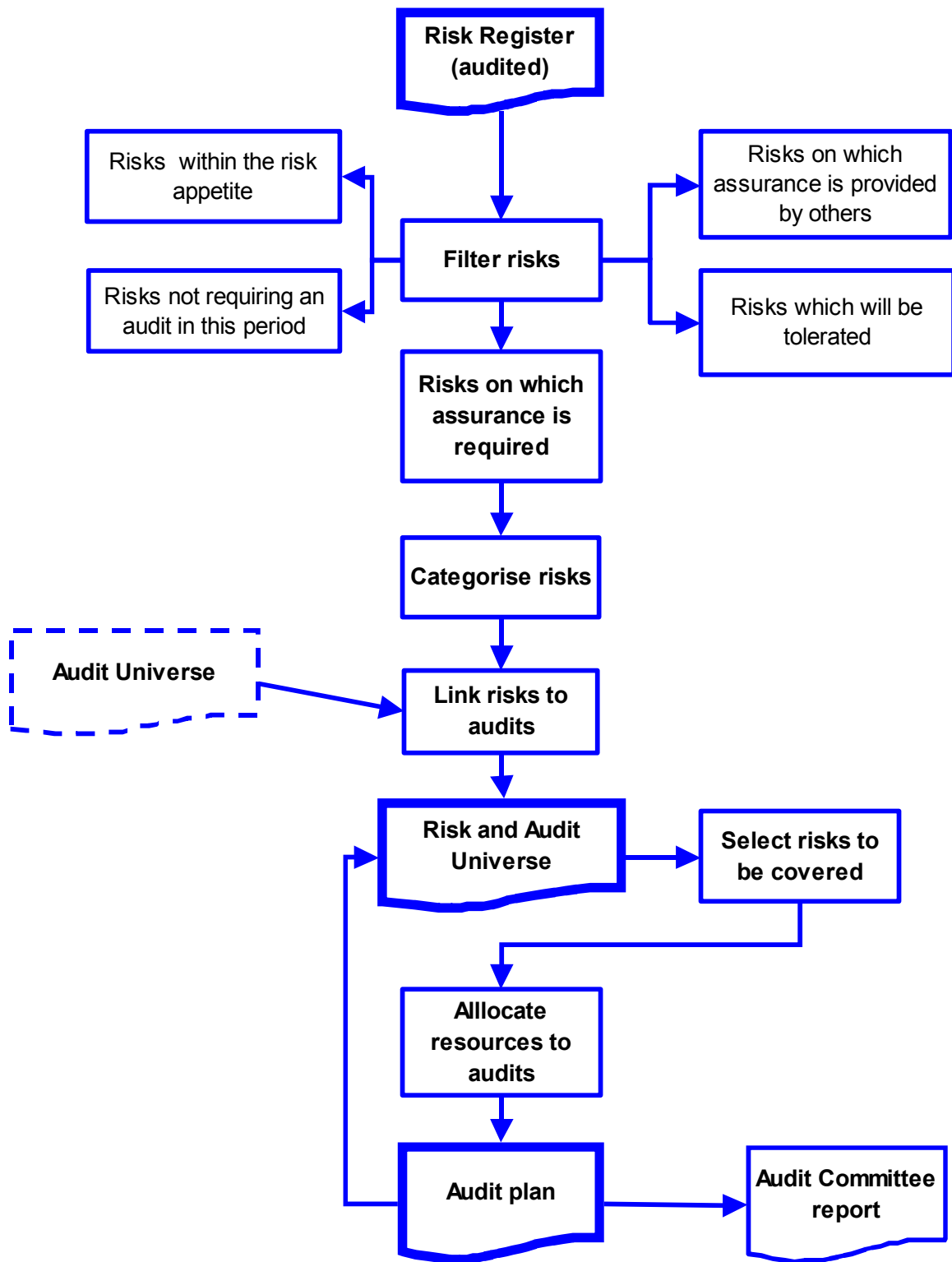


Fig 5 Processes involved in Stage 2

4.6.2 Which risks?

Where risks are to be terminated, transferred or tolerated, a conventional audit will not necessarily be appropriate. Our next stage is therefore to filter the risks as follows:

RBIA – the foundations

- The risk is within the risk appetite of the organisation and requires no further work.
- Management consider the risk cannot be bought within the risk appetite, and it will be tolerated. If contingency plans are required, we do not filter out the risk, in order to ensure the plans are audited.
- Management have transferred the risk, for example by insurance. An audit may still be necessary to ensure all the risk has been transferred. For example that insurance covers all the risks management believes it covers.
- Management will terminate the risk. There may be a need to keep this risk within the audit plan, to ensure that any risks arising from the termination are being managed.
- 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.
- 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.

The remaining risks are those on whose management an opinion is required and these will form the basis of the audit plan (stage 3). 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.

4.6.3 Grouping risks into audits

We now have a risk register from management ([Appendix F](#)) that we can use for the basis of our audit plan. It shows processes, with the risks that hinder them and a score attached to the risk, indicating its significance. (Notes at the end of the appendix provide more details on scoring).

At this stage we could sort the database by risk score to find the most significant risks. However, this will split up the processes so it is useful to group those risks and related processes that will be included in the same audit (I've just used letters – you can be more sophisticated).

The grouping of risks into one audit will depend on:

- The length of time, and resources we want to devote to any single audit (the more processes, the longer it will take).
- The people we wish to interview as part of the audit. (If we are to arrange meetings with many people, we might as well include as many relevant processes as possible).
- The location of the audit. If we are going to Africa, we want to include all the relevant risks and processes.

An alternative method favoured by some organisations is to list out all the possible audits (the *Audit Universe*) first and then link risks and processes to them. This is particularly useful if the organisation has many off-site operations and wishes to audit each one as a unit. If this methodology is used, it's important to check that all risks are being covered by at least one audit.

RBIA – the foundations

Whichever method we use, the risk register will now show the audits that will check their management ([appendix G](#)). The advantage of recording the risk and audit universe by having one line for each risk is that we can sort it by process (sort by columns L1 then L2 then L3) or by adjusted inherent risk score (column S) or in other ways, as we require. (If you need more information look at the 'Managing lists' chapter in the Excel help menu). We can sort the database by the adjusted inherent risk score to give us a long-term plan of the risks on which we will eventually have to provide an opinion.

So we now have a list of risks and the audits (denoted by a letter) that will check the management of those risks (appendix G). This is the start of the *risk and audit universe* that we use as the basis for all our audit work, including the annual plan.

The risk and audit universe attached to my other book on implementing RBIA is basically the same as in this book but has additional columns for how the risk is to be treated and the audit action to be taken.

5 Compiling the annual audit plan

5.1 Objective of the stage

To produce a plan showing:

- Which audits will be carried out.
- When they might be carried out.
- How long they are expected to take (days).
- Which risks and related processes will be included in each audit.
- Who might staff the audits.

The plan will become 'less definite' depending on the length of time to the audit.

5.2 Why an annual plan?

I've heard the proposal that there is no need for an annual plan – since in practice, we can't plan in detail that far ahead. Thus we could work down the risks in the risk and audit universe and build these into a detailed quarterly audit plan. There are however reasons for an annual plan:

- Our organisation's senior management (board, trustees) may require a plan to use as a target for the internal audit activity.
- The Turnbull Guidance requires an annual assessment (para. 27) to ensure that the board has considered all significant aspects of internal control for the year under review. This implies that the annual plan should contain audits which enable the board to make its public statement.

5.3 When to audit?

Is the management of every inherent risk above the risk appetite to be checked every year? Do we have to cover every risk in the first year of setting up RBIA? For most organisations this would require a large number of auditors, so a compromise has to be found.

One possibility is to use our matrix (below). At the start of RBIA we would aim to audit the management of 'red' risks in the first year, 'yellow' risks within two years, 'light green' within three years and 'green' risks never. We can only use this methodology if we are confident in the scoring of the risks.

Likelihood of inherent risk	Rare(1)	1 Never	2 Never	3 Never	4 Never	5 Every three years
	Unlikely (2)	2 Never	4 Never	6 Every three years	8 Every three years	10 Every two years
	Possible (3)	3 Never	6 Every three years	9 Every two years	12 Every two years	15 Every year
	Probable (4)	4 Never	8 Every three years	12 Every two years	16 Every year	20 Every year
	Almost certain (5)	5 Every three years	10 Every two years	15 Every year	20 Every year	25 Every year
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)

Consequence of inherent risk

Fig. 6 Grid for the frequency of audits

It's not ideal. Although it's simple, it reminds me of 'cyclical' auditing, which RBIA is trying to move away from.

5.4 Which audits?

If we don't use the cyclical method above, do we work down to the bottom of the risk and audit universe, before going back to the top, or do we re-audit the controls over 'high' risks before auditing some of the 'low' risks? Our decision depends on:

- The inherent risk score (significance).
- When the audit was last completed.
- The results of the audit.
- The risk level above which the audit committee want our opinion.

We can apply a factor to the risk score, based on the other two. For example:

Time since last audit	3 years	0.75	1	1
	2 years	0.5	0.75	1
	1 year	0.25	0.5	0.75
		Green	Amber	Red

Audit result

Fig. 7 Factors to reduce inherent risk scores

(Audit result: green = risk is controlled, amber = risk is partially controlled, red = risk is not controlled)

So, if the risk has a score of 12, was audited in 2002 and found not to be controlled (red), it would be scored with a significance of $12 \times 0.75 = 8$ when drawing up the 2006 audit plan. (Please bear in mind that I devised this method while eating my lunchtime sandwich – it's only a suggestion!)

So, we take the risk and audit universe (RAU) ([appendix G](#)) we have so far, add details of previous audits to it, and apply the factor to give us the adjusted score for the year, 2006 ([appendix H](#)). This is a more sophisticated system than the cyclical method and does have the important advantage of taking into account the results of the last audit. At this point we now have a means of sorting the RAU by the adjusted inherent risk score to give us risks in order of priority for an opinion on the effectiveness of their management.

We just need to know the value of the adjusted inherent risk score above which the audit committee require an opinion as to the risk's management. This might be the risk appetite score (which we have taken as 4 or below for 'acceptable', that is no audit required). If we 'draw' a line above the scores of 4 and below, any audit above this line should be included in the annual plan. Some audits may involve risks above and below the line and we can decide whether to include these, or not.

In order to uniquely identify a specific audit, an audit number is added from the top (starting from last year's last number) and put against each risk in that audit letter. An alternative numbering method would be to use the audit letter and year of audit as the identifier (For example, D2004). It is at this point that we might wish to omit the lower scored risks from audits. If we were using a proper database (as opposed to a spreadsheet) we could link details of the audits carried out to the processes, using the unique audit number.

RBIA - Compiling the audit plan

There are alternatives to the approach used above. For example, if the number of risks is large, it is probably better to group them into audits and then score each audit, based on the risks included. Each audit could be scored on the total risk score it included, or the average. Make your choice!

We do need to add the process owners, since it is they who are accountable for delivering the output from their process, and who therefore own the risks. They are our main points of contact.

5.5 Resources

We can decide on the staff resources required to deliver the audit plan by deciding on the number of days each level of auditor is required for each audit, adding these up, and comparing them with the total days available. This calculation is done at the bottom of appendix H of the Excel spreadsheet. (We could of course work out the resources available first and see what audits we can carry out but this is not recommended as a basis for providing an opinion on the control over the organisation's risks).

Note that audits will vary in length, even those which are high risk could be done very quickly. It may only take logging into our organisation's intranet to confirm that it has a strategy, and this is being communicated.

The resource requirements should be regularly updated to ensure the plan can be completed, especially if audits are added and staff leave.

5.6 The ongoing risk and audit universe

We now have the **definitive risk and audit universe** of processes, risks and audits for 2006 ([appendix H](#)). This database is used to:

- Record the processes and their related risks. It is updated at least quarterly by those managers who own the processes.
- Show the 'owner' of the risks, that is the person directly responsible for ensuring the risk is being properly managed. It is likely to be this person who carries out the monitoring controls.
- Decide on those risks, with management, where it requires audits to give an opinion whether the risks are being managed to acceptable levels. This includes the addition and removal of audits resulting from the periodic updates of risks and their scores.
- Show the risks whose management will be checked by each audit.
- Indicate the agreed timing (month or quarter) of planned audits.
- Show the status of the audits for the current year (unplanned, planned, fieldwork, reporting, complete).
- Indicate the achievement of milestones (agreement of the work required, report).
- Show the results of previous audits.
- Form the basis of next year's plan, after updating with the results of audits from this year.
- If required, show the controls and monitoring controls which manage the significant risks in the RAU. These will otherwise be shown in the individual audit databases.

5.7 Publishing the annual plan

We've now got an annual plan within the RAU ([appendix H](#)), which can be sorted or filtered to provide a variety of reports. This spreadsheet is so wide, only part is included in appendix H. I would advise you to download it from www.internalaudit.biz.

We will provide the audit committee with a summary which will show:

- Details of those risks where an opinion will be provided about the risk management processes by carrying out the audits in the plan.
- Details of those risks where an opinion will be provided but based on audit work from previous years, plus limited follow-up work where desirable.
- Details of those risks where consultancy work will be carried out to assist management in reducing the residual 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.

5.8 Quarterly plan

In the good old days when we had work plans which defined clearly what tests should be done, and management were involved only in the close down meeting, we knew exactly how long an audit would take and people could work full time on that audit.

Risk-based audits are not so simple:

- We may never have audited these processes before and can't easily estimate the time required.
- We are auditing strategic processes, which involve strategic people, who aren't always available. Even meetings that are arranged well in advance may be cancelled at short notice, leaving the auditor short of work. (OK, I know internal audit should be so important that directors won't cancel meetings, even when the CEO calls them).
- Risk workshops and close down meetings will have to be arranged well in advance, and even then we may lose one or two important persons, so delaying the audit.

My experience of managing risk-based audits is that, in order to ensure auditors are kept busy, they need at least three audits – one being set up, one where fieldwork is being done and one where the report is being written and agreed. You can also throw in a systems development audit. This requires the recruiting of self-motivated auditors who can prioritise their time – but that's another story.

An example of the quarterly plan is in [appendix I](#)

6 Providing the opinion

6.1 Objective

To provide an opinion as to whether the risks covered by the audit are being managed to within the risk appetite. The processes involved are shown below.

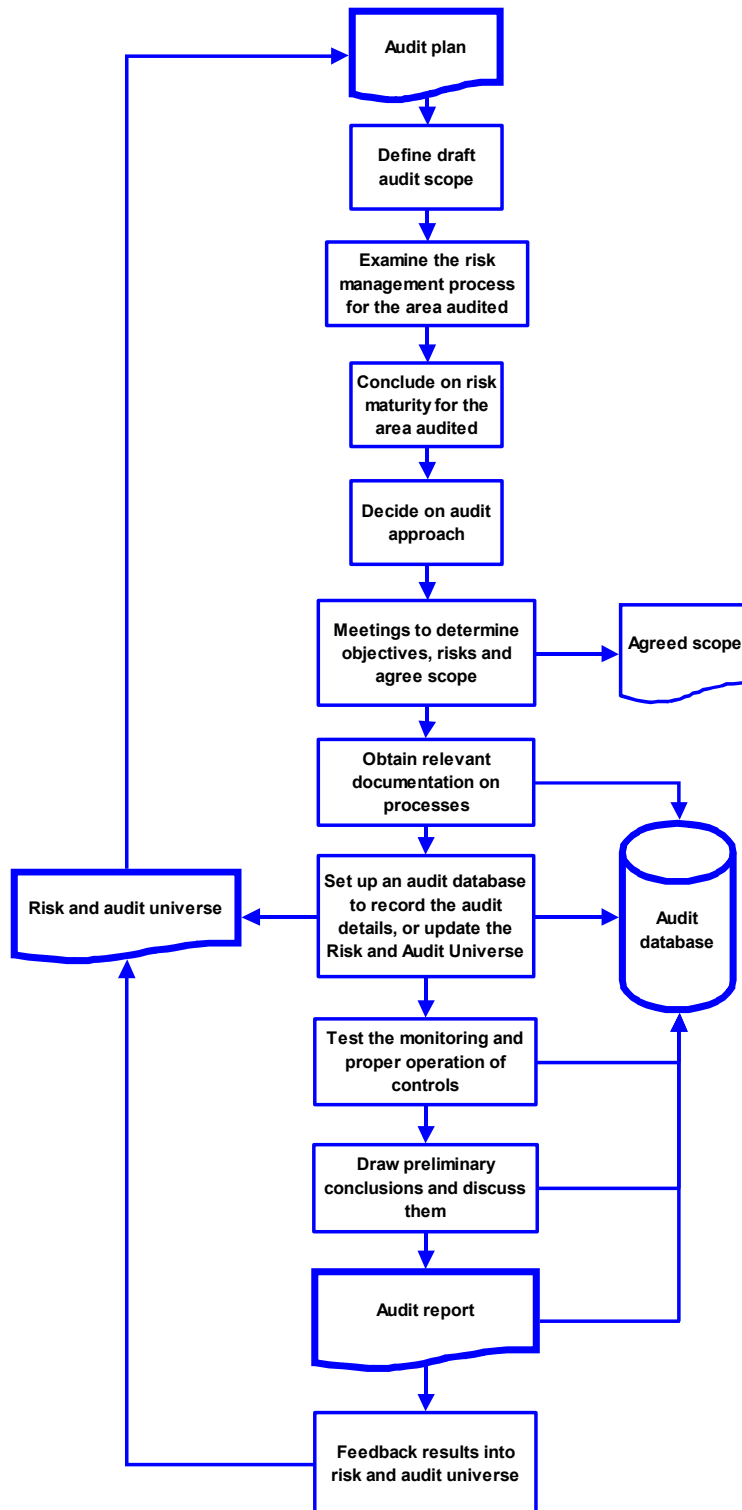


Fig 5 Processes involved in stage 3

This figure is also provided on an Excel spreadsheet in the file to be used with this book.

6.2 What is an audit?

So, we know what audits we're doing, when we're doing them and who's doing them, even if we don't know precisely how long they will take. We also know, at a high level from the plan, the risks on whose management we will provide an opinion and the high level business processes which these risks are threatening.

So how do we do the audits? Back to first principles: internal auditing provides an opinion to management whether *risks*, which hinder the achievement of *objectives and processes*, are being managed by *internal controls*. So the basic structure of an audit is:

1. Determine, in greater detail than is probably in the plan, the processes which deliver the high level objectives.
2. Check the risk management framework in the areas concerned, using the methodology in stage 1. Where the organisation has not determined its detailed risks, you have choices:
 - Stop the audit work and report to senior management that it cannot continue because management have not identified risks.
 - Work with the management to identify and evaluate the detailed risks affecting their processes.

Document all risks and associated processes in an audit database ([appendix K](#)). The definitive list of risks is noted in the column 'risks for this audit'. The more risk mature the organisation is, the more information will be available on risks and their associated controls.

3. Ascertain, and test the existence of, the internal controls. The greater the risk maturity, the greater the emphasis will be on checking the monitoring controls carried out by management. Check the residual risk scores evaluated by management, on the basis of the test results. If they have not been scored, agree a score with management.
4. Decide where risks are not being sufficiently managed by controls, according to the organisation's risk appetite.
5. Provide an opinion to management whether individual risks are being managed to an acceptable level. Agree the action to be taken, and timing, with management.

The diagram in [appendix J](#) shows 5 stages involved in an individual audit in relation to the overall purpose of internal auditing.

In practice audit stages 1 and possibly 2 will be included in the planning stage, and staff probably won't be engaged full time on this audit. Stages 2,3 and 4 will form the fieldwork stage of the audit, when staff are likely to be full time. Stage 5 is the reporting stage.

The practical processes for carrying out an audit are shown in the *operational manual for risk-based audits*, available from www.internalaudit.biz. The notes below provide more details about the audit processes.

6.3 Planning - the audit scope

The purpose of the scope document is to set out *why* the audit is being done, *what* risks and processes it will involve, *what* it will deliver, *how* it will deliver, *who* will deliver and *when* they will deliver. We will send it to every manager who has an interest in the audit, with a request to brief his or her staff.

Where possible, we should provide figures to emphasise the monetary value at risk. This could include not only potential losses but also 'loss of opportunity'.

The scope must state the *processes* being covered; ideally relating them back to the agreed process map. If any processes are specifically excluded from the audit, this should also be stated. There is a tendency for people to assume the area of an audit is always larger than it actually is. In other words – we need to manage expectations.

We need to note the objectives of the processes being audited (*not* the objectives of the audit). This is important, since our audit will be providing an opinion on whether the risks threatening the processes are being properly managed. If they are not, the objectives will not be achieved.

The scope therefore, will have the following headings:

- The reasons for the audit.
- The objectives, risks and related processes and key controls
- The work programme, which should follow the approved methodology.
- Factors which define the limits of the audit including processes specifically excluded.
- Any special considerations, such as management requests, provided they are acceptable.
- The personnel carrying out the audit, including any special responsibilities.
- The timing of the audit.
- The recipients of the scope, draft and final report (although these may change, depending on the issues found by the audit).

The reasons for the audit should include the objectives of the audit, that is, to conclude on whether:

- Risks have been properly identified, evaluated and managed.
- Internal controls are operating properly to mitigate these risks to levels defined as acceptable by board policy.
- Action is being taken to improve controls, where risks are not being properly managed.
- More monitoring, by management, is necessary to ensure proper internal controls into the future.

The scope will be agreed with our 'customers' – although we, the auditors, have the final say! A meeting to discuss the scope is a good opportunity to get everyone, auditors and people affected by the audit, together.

As the audit progresses, we may wish to change the scope. This should be done as soon as possible, in conjunction with those who agreed the original scope.

6.4 Fieldwork - fact-finding and risk assessment

This stage involves finding out, using interviews and following through transactions to see how the detailed processes work. Don't lose sight of our aim, there is no need to devote time to minor risks and document processes in fine detail.

RBIA – Providing the opinion

We may be outside our 'comfort zone' in this type of audit. It is important to remember that we are not trying to do the job of those people who are using the processes we are auditing. We are there to provide an opinion whether management have identified their risks, and are operating controls to manage them. If we don't think we have the expertise to do this, we should be bringing in help from specialists inside, or outside, the organisation.

Fact-finding often overlaps with risk and control assessment. Feedback from my customers indicates that, during these stages, they like to be involved through meetings where they can have the audit explained to them and get the chance to raise issues. These meetings, which could be used as risk workshops, are also very useful as they encourage buy-in from everyone involved.

Fieldwork serves two purposes:

- Determining the risk maturity of the areas concerned – have they identified and evaluated risks, are they operating a system of internal control to manage them?
- Ascertaining the internal controls which manage the risks. Two types are noted in the audit database:
 1. Direct controls – those that address the risk directly, such as authorisation of invoices, bank reconciliations.
 2. Monitoring controls – those processes operated by management to ensure key controls are operating effectively, such as approving the bank reconciliations, scrutinising the overdue debtors listings.

6.4.1 Risk maturity

Hopefully, we will collect a detailed list of risks from the managers involved, or the organisation's main risk register may be sufficiently detailed. Where risks have not been determined in detail, and we have decided to proceed with the audit, we will determine risks from risk workshops (appendix E), meetings and best practice guidelines

Risks will be put into a database and scored (appendix K). This database breaks down the main processes identified in the scope, and therefore contains the next level(s) below those in the risk and audit universe. It would be possible to incorporate these in the risk database, but for most companies this would result in a large database which would be difficult to manage.

The example in [appendix K](#) is for the audit of processes 4.2 and 4.3 (grouped into audit K – *Transport of food to camps*, audit number 146).

The risks we identified in level 2 as part of the initial risk assessment should be incorporated into the audit database, but may need to be amended. The process of risk assessment is one of continual update.

The audit database is the central information source for the audit. It can contain most data related to the audit, and be hyperlinked to notes of meetings and other documents. Thus, we have not only set up a document management system, we have abolished much of the documentation used in a 'traditional' audit!

Risks that are present in most processes should also be considered (contingency, competencies, fraud – details in [appendix L](#)). These have been added into the audit database as appropriate.

6.4.2 Ascertaining controls

Those processes which control risks will be noted in the audit database, as will those processes which monitor the proper operation of the controls.

RBIA – Providing the opinion

Sufficient detail should be recorded so that the residual risk score can be checked, and the control's operation can be tested. This applies to direct controls and monitoring controls.

6.5 Fieldwork-testing controls

The existence of controls will be checked, paying particular attention to those which have a significant effect on inherent risks, that is they have a high *control score* (inherent risk score less residual risk score). The types of tests used, for example compliance, reconciliation, computer assisted, will be no different from those used in financial-style audits and so I'm not providing details. The aim may be slightly different in that the tests are designed to prove the existence and proper operation of internal controls, NOT to find errors.

The emphasis of testing will depend on the risk maturity of our organisation. If it is highly mature (risk enabled) we should have the confidence that management have implemented good internal controls and we can concentrate on testing their monitoring of these controls. For a less risk mature organisation (risk defined) we will spend more time looking at the direct controls as well as the monitoring controls.

Internal auditing is not part of the day-to-day control process, but to draw a conclusion as to how controls have operated to manage risks in the past, in order to draw a conclusion as to how successfully they will manage risks in the future. The important question to ask is, "If these controls fail in the future – how will *management* know?" (This is why the Turnbull guidance requires an opinion on monitoring.)

The managers with whom we are working should be provided with a report showing processes, risks and controls, and asked to confirm the existence of these controls. This can be done as an appendix to the audit report ([appendix M](#)).

6.6 The opinions

This is the difficult bit – assessing whether the risks are being properly managed by the system of internal control.

The score of the *residual risks*, re-assessed after our testing of the controls actually in operation, should be our guide, and the chart below is similar to that we have used for inherent risks.



Consequence of residual risk

Unacceptable: Immediate action required to control the risk

Issue: Action required to control the risk

Supplementary issue: Action is advisable if it is cost-effective

Acceptable: No action required

■ ■ ■ ■ ■ Risk appetite, as defined by the board

Fig. 9 Grid for the significance of residual risks

This chart implies:

- A residual risk scoring 15 or above, is 'unacceptable'. The risk is not being managed to an acceptable level by the control(s) and it is probable that some objectives will not be, or are not being, achieved (red).

RBIA – Providing the opinion

- A residual risk scoring 9 or above is an 'Issue'. The risk is not being mitigated to an acceptable level by the control(s). There is the possibility that some objectives will not be achieved.
- The grading of a risk with a score of 5 or above (that is one with a high likelihood or consequence and low consequence or likelihood) is difficult. In practice, it may not be possible to manage and it has to be accepted (green). If there are cost-effective controls which can mitigate it, then it is considered a 'supplementary issue' in the report.
- A residual risk scoring 4, or below, falls within our risk appetite and is 'acceptable'. The risk is being mitigated to an acceptable level by the control(s) and no further action is required.

We are now able to form a preliminary opinion on the management of each of the risks, from the following options:

- 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.

Where residual risks are above the risk appetite, these will be listed for discussion with management. The opinion on each risk will determine the overall conclusions.

Where we are reporting 'unacceptable risks', or 'issues', should we make recommendations as to how these can be reduced to acceptable risks?

Theoretically, since management are responsible for implementing controls, we should not need to provide recommendations – they should put forward their solution to us. This will happen with risk enabled and risk managed organisations, but with risk defined organisations they may want advice. This should go under the heading of 'consultancy'. This issue is discussed in more detail in the section on the benefits of RBIA.

Appendix K shows the detail for the audit. Since it is a long spreadsheet, I suggest you download it from the web site (www.internalaudit.biz).

6.7 Reporting to management

There are various points in an audit when we need to report the issues found back to management. Risk-based audits are no different from any other audit methods, although the format may be slightly different.

6.7.1 Update reports

We should have kept the managers (of the processes being audited) informed of progress throughout the audit, particularly if significant risks were found. This gives them the opportunity to implement additional controls as soon as possible and avoids nasty surprises at the close down meeting.

6.7.2 The close down meeting

We will hold a 'close down' meeting, with all interested parties, to discuss those residual risks above the risk appetite and any other issues found during the audit. The outcome from this meeting is a record of the action management will take to bring risks within the risk appetite, or risks they will terminate, transfer, or tolerate. These last three risks should be included in our 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, we will check the existence, and testing, of any contingency plans, where possible. We should have discussed any contentious issues before this meeting to ensure 'no surprises'. It is important that we start this meeting by stressing the good points that we found during the audit.

If we agreed with management at the start of the audit, those risks which hinder the objectives of the processes, and the controls actually operating, there should not be too much discussion over whether risks are being properly managed. (That's the theory anyway!)

6.7.3 The report

The primary aim of the report is to conclude whether the risks hindering the achievement of those objectives and processes noted in the scope, are being managed to an acceptable level. The report is the highly visible 'product' of our internal audit department. It must not only achieve the above aim but must be clear, concise, free from grammatical and punctuation errors, well designed and relevant.

The Turnbull guidance (2005) states:

Paragraph 29: The reports from management to the board should, in relation to the areas covered by them, provide a balanced assessment of the significant risks and the effectiveness of the system of internal control in managing those risks. Any significant control failings or weaknesses identified should be discussed in the reports, including the impact that they have had, could have had, or may have, on the company and the actions being taken to rectify them. It is essential that there be openness of communication by management with the board on matters relating to risk and control.

Paragraph 30: When reviewing reports during the year, the board should:

- *consider what are the significant risks and assess how they have been identified, evaluated and managed.*
- *assess the effectiveness of the related system of internal control in managing the significant risks, having regard, in particular, to any significant failings or weaknesses in internal control that have been reported.*
- *consider whether necessary actions are being taken promptly to remedy any significant failings or weaknesses.*
- *consider whether the findings indicate a need for more extensive monitoring of the system of internal control.*

Since these seem sensible aims, I suggest that individual reports should have a conclusion against each, plus an overall conclusion as required by the IIA Framework. These can then be easily summarised for the annual report to the audit committee.

The conclusion for each of the four aims above is graded.

- 'Unacceptable' (red): significant weaknesses that prevent the aim being achieved.

RBIA – Providing the opinion

- ‘Issues’ (amber): some weaknesses which might prevent the aim being achieved.
- ‘Acceptable’ (green): Minor, or no, weaknesses and the aim is being, and will continue to be, achieved.

The grade is determined by considering the opinions made against each of the risks. For example, if there are any risks with the opinion ‘The risk is not being managed to within the risk appetite, and no suitable action is being taken.’ then the conclusion on the effectiveness of controls is likely to be ‘unacceptable’. The audit manual (section I – draft report), and related database, provide more details.

Our overall conclusion will depend on all the results from the audit – there is no simple formula. For example, the conclusion on processes which have only one significant risk, which is being immediately addressed by management may be an ‘amber’. However, the conclusion on processes which have no ‘reds’, but many ‘ambers’, which the management are totally ignoring, may be a ‘red’.

How you report your conclusion will depend on your organisation. Some like the report to be given a numerical score – depending on how good the controls are. Comments from auditors who have to use this method suggest it should be avoided, as much time is spent haggling over the score and not enough time on controlling the risks!

Reports can be in four parts, reflecting the findings of the audit:

1. **Executive Summary**, containing the conclusions, actions to be taken (if any), reasons for the audit and the objectives and risks of the processes audited. Sent to the audit committee, main board directors (or trustees or owners), business directors responsible, managers directly involved.
2. **Key issues**, (these result from red or amber risks) detailing the risk, the consequence if the risk event occurs, recommendations for lowering it to an acceptable level (if appropriate), actions to be taken, by whom and when. Sent to business directors responsible, managers directly involved.
3. **Supplementary issues** (these result from green risks which can be further reduced by simple cost-effective measures) detailing the risk and consequences if it occurs. Recommendations (if appropriate), and action to be taken will depend on the issue. Sent to managers directly involved.
4. **Processes, risks and controls report** ([appendix M](#)). Sent to managers directly involved. This report, derived from the audit database, can be long but has several advantages:
 - It shows the work that the auditors have done to support their conclusions. This is especially useful if the auditors worked for two weeks and came up with a two page executive summary giving a ‘green’ conclusion!
 - It can put any significant risks into context. If we have found one significant uncontrolled risk out of 20 properly controlled key risks, the manager concerned can point to this when talking to his/her boss about the report. (Because audit reports tend to stress the negative, I am considering whether it is possible to give some measure in the executive report – such as “95% of key risks are well controlled”).
 - It provides managers with a list of processes, risks and controls. Thus, if they wish to change their systems in any way, they can see how they might affect their residual risks. Similarly the auditors can see the effect of any changes.

6.8 Projects

The audit of projects, for example the implementation of a new computer system, is different from the risk-based audit of an ongoing system for two reasons:

1. The timescales are much longer. An audit of a major project would last over its life, possibly several years.
2. An opinion is required whether that the following risks are being managed:
 - Risks hindering the project from delivering the objectives on time and within budget.
 - Risks which will be present from day one of the project implementation (for example when the system goes 'live')

The identification of risks hindering the project should be relatively straightforward; for example, we can hold risk workshops with the project team. These should help us identify most risks, but we will have to update the risk database every month, to take account of risks changing as the project progresses. For the same reason, we will issue a brief report every month, assuring management that risks are being managed, reporting those that are not and indicating the action being taken.

The risks that will be present when the project is implemented are more difficult to assess. For a start, we are unlikely to know the controls which will be in place, in fact we'll probably have to advise on them. It's difficult to maintain objectivity here, but we can hardly refuse – since we're meant to be the experts! However, in a large project, the team should have their own control experts – leaving us to assure management that they are operating properly. In practice, the least we should expect in the early stages of a project is a process map with risks attached and possible controls. As the project progresses this should become more detailed, until it resembles our audit database. As with the project risks, we should issue regular monthly reports.

6.9 Stage 5 - Report to the audit committee

Both the Turnbull guidelines in the UK, and Sarbanes-Oxley in the US, require an 'annual report' from management on the effectiveness of internal controls. The frequency and contents of the report to the audit committee will depend on the internal audit activity's charter but will normally include:

1. Opinions on whether
 - The significant risks have been identified, evaluated and managed.
 - The related system of internal control has been effective in managing the significant risks, having regard, in particular, to any significant failings or weaknesses in internal control that have been reported.
 - Necessary actions are being taken promptly to remedy any significant failings or weaknesses.
 - The findings indicate a need for more extensive monitoring of the system of internal control.
2. The audit plan, agreed with the audit committee at the start of the year, has been achieved. If it has not, why not. (If the report is an interim one, the progress towards achieving the plan).

7 What is the impact of risk-based auditing?

7.1 How the delivery of internal auditing is changed

One major change is demonstrated by the audit report. 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 internal audit is to clarify its role:

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

Where the opinion states risk management to be ineffective, 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:

If no risk management framework is in place (risk naïve or risk aware organisations) risk based internal auditing cannot be carried out as there is nothing on which to base the audit work. Only consultancy work to facilitate the implementation of a risk management framework is possible.

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.

The change to a risk-based approach is a fundamental change which affects the delivery of internal auditing from start (planning the audits) to finish (report), and all stages in between (staffing, time budgets, field work).

The biggest change is the relationship with the rest of the organisation – it has to play a major part in all stages of the audit. This is hardly surprising, since it owns the risks on which the audit process depends.

We can only talk about the change *to* risk-based auditing if we know what it is changing *from*. That's not easy, since there are many different way of delivering internal auditing at present. The best way of seeing what is happening is to type 'internal audit' into a search engine and look at the sites it finds.

RBIA – The benefits

We can summarise the change below, although this involves some assumptions regarding 'Previous Methodology':

Audit process	Risk-based auditing	Previous methodology
Audit universe	All activities of the business	Primarily financial areas but also involving compliance with laws and regulations, and 'operations'
Audit objective	Provide an opinion as to whether risks are being managed to acceptable levels	Confirm internal controls are operating. Improve efficiency
Annual plan	Audits directed at high risks	Cyclical plan of audits, not necessarily dependent on risk levels
Audit types	Only distinction is between project (systems development) audits and ongoing processes	Distinguishes between financial, operational, compliance and other types
Involvement of the rest of the organisation	Involved at all stages of planning and the audit, since they own the risks and must provide assurance to the stakeholders	Minimal. May approve the audit plan and be involved at the end of an audit to agree the points found
Staff plan	Several audits allocated to one or more staff at any one time	One audit allocated to one or more staff
Time budgets	Difficult to set. May be a first-time audit, or one where systems have changed	Easy to set – since the audit has usually been done before
Fieldwork	Ensures the organisation has identified all its risks, and is controlling them	Based on a set work programme, where there may be no clear objective set, just tests to carry out
Testing	Similar tests as used at present but aimed at confirming that important controls are operating. Changes emphasis of testing depending on risk maturity of the organisation.	Confirms the operation of controls – but may not prioritise these in order of importance. May also be directed towards finding errors, however immaterial.
Report	Provides an opinion to management as to whether <i>its</i> risks are being managed to acceptable levels, and reports if they are not	Confirms internal controls are operating and reports where they are not

RBIA – The benefits

Audit process	Risk-based auditing	Previous methodology
Recommendations	No recommendations are made as management have responsibility for deciding on the internal controls required. Any recommendations made are part of a consultancy exercise.	Recommendations are made to correct weaknesses found
Annual report to the 'board'	Provide an opinion as to whether risks are being managed to acceptable levels. Can give an indication as to the proportion of risks covered	Confirms that the audit plan has been completed, and highlights controls not operating. Cannot give any indication as to the proportion of significant risks covered
Staffing	Self-motivated, experienced staff used to working with senior management. May be specialists who are not accountants, and may be seconded.	Usually accountants and career internal auditors

7.2 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:

- 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 close-down 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 which are not properly managed.

The impact of this greater involvement by management is:

- The Head of Internal Audit (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 which managers can understand and, hopefully, support.

RBIA – The benefits

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.

7.3 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.

7.4 Management of the 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.

7.5 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 come to an opinion on the management of risks covered by the audit.

Specialist knowledge may be acquired as follows:

- We use specialist skills available in our internal audit activity. For example, the knowledge of computer auditors where controls over access to a computer system require verification.
- We provide specialist training to our auditors who have 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 our external auditors.
- We recruit specialists from inside our 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.

- We use specialists from outside our organisation. For example health and safety experts to audit our health and safety processes. Although such specialists may work on their own, they should follow our audit methodology and the scope of the audit should be clearly defined. Their audit documentation should meet our standards, and be reviewed to ensure it meets the quality we expect.

7.6 The benefits

The benefits of risk-based auditing are considerable:

- Risk-based auditing is a simple concept. There is no need for a complex definition of internal control, or internal auditing, and it involves the whole organisation and its processes – so no need to define which functions internal auditing should involve – all of them.
- Alongside this simplicity, there is a unity. The recommendations made can be traced back through controls, risks and processes to the organisation's objectives, using the RAU and audit databases. Similarly, we can easily demonstrate what proportion of significant risks we have audited, and the results, to provide assurance to the board about the “effectiveness of the company’s system of internal control” (LSE Combined Code). RBIA ties all aspects of internal auditing together; objectives, processes, risks, controls, tests and reports (see diagram in section 4.4.4). 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.
- The organisation buys in to the audit process. Because it has to be closely involved in the process, and should be able to clearly see the benefits of our output, it is far more likely to support the audit work, as opposed to treating it like an unwanted imposition. (No-one does that – do they?).
- Resources can be justified. 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 which can be carried out. It also ensures that resources are directed towards checking the management of the most significant risks
- The work is more challenging and interesting to staff. They have to work in non-finance areas, with staff that may be seconded in for the audit. There is no handle-turning of work programmes, without really understanding why the test is being done.
- Risk-based auditing is more efficient, because it directs audits at the high-risk areas, as opposed to financial areas, which may not represent such a great risk.
- We can rank recommendations, to provide the greatest value added in terms of the risks mitigated.
- RBIA should highlight risks which are over-controlled, and therefore improve efficiency

RBIA – The benefits

Fundamentally, the internal audit function is now much more part of the organisation and less introspective. It involves the organisation more in the audit process and produces recommendations which contribute to its objectives. At the same time it has to be careful not to lose its independence and objectivity, as a result of getting closer to the operations.

7.7 Disadvantages

With every advantage there are always some disadvantages:

- The closer relationship with the rest of the organisation may reduce the independence of the internal audit function. We should prevent this by making the responsibility of internal auditing clear and by adopting the 'iron fist in a velvet glove' approach.
- It's hard work! We have to sell the risk-based process to the organisation, get it to tell us its risks, score them and then have to carry out some difficult audits which we have never done before! Stakeholder management is vital, and takes time.
- While the principles are simple, the delivery can be complex, as we can see from the spreadsheets.
- Existing staff may need retraining.
- By concentrating on audits of inherent risks above the risk appetite, some audits previously considered important by senior management might disappear. These might include audits of small overseas subsidiaries, 'petty cash' and the Staff Social Club.

7.8 Some questions

7.8.1 What happened to the consultancy responsibilities of internal auditing?

I believe that the activity of internal auditing should be solely directed towards providing an opinion, and fulfilling the requirements of the LSE or Sarbanes-Oxley. To include consultancy changes the focus of the activity, and could be a contradictory aim, in some cases.

This does not mean that internal audit activity doesn't give advice on the controls to be expected, or facilitate the identification of risks but this role must not hinder the primary objective.

7.8.2 Do I have to throw away my work programmes and questionnaires?

Ideally – yes! The danger of using programmes are :

- They can be incomplete. In particular, they might not check the management of all significant risks.
- Since many are not linked to risks, there is no indication as to the importance of the test and the consequence if the control tested is found to be ineffective.
- They can lead to a 'box ticking' exercise by staff anxious to hit the budgeted time, without gaining an understanding of what they are doing. In this way, major risks which are not being managed properly may be missed.
- They don't encourage management to identify and control their risks.

RBIA – The benefits

The only reason for retaining them is to act as a useful checklist to ensure we have identified all the risks and controls for the processes we are auditing.

I hope in future that published work programmes will disappear, to be replaced by lists of typical risks and controls.

7.8.3 Do financial audits disappear?

No, but the risks included in these audits have to be judged alongside all the risks faced by the organisation. Which is the more important, the failure to get food through to famine areas because lorries have broken down, or an incorrect calculation of depreciation?

7.8.4 Where does Control Self-assessment (CSA) fit in?

I have great doubts about CSA. I have used it, and seen it fail to achieve its objectives. There is a fundamental contradiction:

- Conscientious managers will always be aware of the limitations of their systems, and are likely to answer “No” to some questions.
- Managers who don't really care about controls will just answer, “Yes” to every question.

So what do you audit? The processes with some “No” answers or those with all “Yes” answers? If you still have any doubts, consider this question from a CSA form, ‘Unreconciled financial transactions are researched and corrected in a reasonable period of time’. Who is going to answer “No” to that question?

I know that the defence of CSA is to say that it must be backed up by audits and disciplinary action, but that only disguises the fundamental problem.

So is all lost? No – look at the problem from the point of view of a manager:

- Help them to identify the significant risks they face
- Agree the controls necessary to mitigate these risks
- Advise on tests, which the manager can carry out (or ask his/her staff to carry out) which proves the control is working.
- Put these on a questionnaire for staff to confirm, monthly, to the manager, that the controls are operating. (So no opportunity for a “No” answer!). Put this confirmation in their job targets.
- Tell the manager to file the document. It is his, or her, responsibility to ensure risks have been identified and are being controlled, not ours.

The internal audit activity can confirm the correct operation of this procedure as part of its risk-based agenda.

I have used this procedure as a manager of an accounting department (100 staff) and it works. It would also form useful evidence to support Sarbanes-Oxley requirements.

7.8.5 What's Enterprise Risk Management (ERM)?

Sometimes known as Enterprise-wide risk management (EWRM). It has been defined as:

“A structured 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” *The role of internal audit in enterprise-wide risk management* IIA – UK and Ireland

RBIA – The benefits

It is no different to the approach that we have seen in this report, it's just that if you are a bank, or chemical company, it's a lot more complex. A bank will have credit risks and a chemical company will have environmental hazards. Both will probably have specialist departments to ensure these risks are managed. The role of the internal audit activity may be to provide an opinion as to whether these specialist departments are ensuring effective risk management. However, the Board may decide to obtain assurance directly from these departments. These danger of this approach is that risks may fall between the various areas of responsibility.

COSO have also produced a standard for ERM, which is very long.

Ernst & Young have looked at risk from the shareholders' point of view (see chapter 9) and produced a hierarchy in a similar way to this report.

7.8.6 What about the COSO framework?

COSO is the abbreviation for the 'Committee of Sponsoring Organisations' and in 1987 it sponsored a commission under the chairmanship of James A. Treadway to produce a report 'National Commission on Fraudulent Reporting'. It sets down recommendations to prevent fraudulent financial reporting, including, "all public companies must have an effective and objective internal audit function". The fact that its recommendations didn't stop Enron's or WorldCom's collapse says more about corporate culture than about the report's effectiveness.

The Committee also commissioned 'Internal Control – integrated framework', which is considered, in the US, an important standard for internal audits. I find it rather prescriptive compared to risk-based auditing.

See chapter 9 for the web address of a briefing paper.

7.8.7 Where do fraud investigations fit in?

Theoretically the consequence and likelihood of frauds occurring in all processes should be considered and, if this results in a high-risk score, that risk will be audited. Unfortunately frauds are rather emotional, often small frauds resulting in a reaction out of proportion to their loss. This is not surprising, since they often represent a betrayal of trust which makes everyone around feel ashamed. There may therefore be a need to artificially inflate the consequence score to recognise this.

Otherwise the detection of fraud is management's responsibility. Similarly, 'embedded monitoring' carried out by the internal activity is work management should be doing. If management like the results from CATTs (computer aided audit techniques), tell them where to buy a copy of the program.

8 Glossary

Beware – these are not ‘official’ definitions!

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

Board: 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: a process which manages a risk.

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.

Facilitating: Working with a group (or individual) to make it easier for that group (or individual) to achieve the objectives that the group has agreed for the meeting or activity. This involves listening, challenging, observing, questioning and supporting the group and its members. It does not involve doing the work or taking decisions.

Inherent (gross) Risk: a risk evaluated without any responses being taken into consideration.

Internal auditing: provides an independent and objective opinion to an organisation’s management as to whether its risks are being managed to acceptable levels.

Internal audit activity: the function (department) which delivers internal auditing to the organisation. It may also be responsible for other activities such as providing accounting staff to cover vacancies and facilitating risk management. It will usually consist of internal audit staff, managed by a Head of Audit (HIA), governed by a charter established by the organisation’s audit committee.

Internal control: a term usually used to indicate the response to a risk, the options being; terminate; transfer; tolerate; treat.

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.

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

Process: a task which assists in delivering an organisation’s objectives (for example, despatch of goods), or controls risks (authorisation of invoices), or provides a risk framework (identifies risks).

Residual (net) Risk: a risk evaluated with any responses being taken into consideration.

Risk: a set of circumstances that hinder the achievement of objectives.

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.

RBIA – Glossary

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

Risk based internal auditing: see 'Internal auditing'!

Risk Management Framework: all the processes which aim to identify, assess and manage risks.

Risk Maturity: An assessment of how well an organisation understands its risks and is managing them.

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

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

9 Useful information

In order to link to the web sites below, you will have to use the electronic version of this document, or log onto www.internalaudit.biz.

9.1 *Audit and accountancy institutes*

9.1.1 Institute of Internal Auditors (U.S.)

This site (www.theiia.org) has a wealth of information – though it's not always easy to find (click 'Guidance' on the top menu).

Direct links:

[Code of ethics](#)

[Standards](#)

[Setting up an audit department](#)

[Sarbanes-Oxley Act \(part\)](#)

9.1.2 Institute of Internal Auditors (U.K.)

This site (www.iaa.org.uk) has a useful '[Knowledge Centre](#)' plus links to U.K. documents.

[An approach to implementing Risk Based Internal Auditing](#)

[Bulletin – Independence and objectivity](#)

[Position statement on risk based internal auditing](#)

[Position statement on the role of internal audit in enterprise –wide risk management](#)

[Deloitte & Touche and the Institute of Internal Auditors – UK and Ireland \(IIA\) 'The value agenda'](#)

[Embedding risk management into the culture of your organisation](#) (details of how to obtain the briefing note)

9.1.3 The Institute of Chartered Accountants in England and Wales (ICAEW)

The institute (www.icaew.co.uk) has several useful documents. From the home page, select 'Policy' on the left index and then 'Risk management and reporting'.

Direct links:

[Implementing Turnbull – a boardroom briefing](#)

9.1.4 The Association of Chartered Certified Accountants

Their site has an [internal audit bulletin](#)

9.2 Official standard setting organisations US

9.2.1 Public Company Accounts Oversight Board

Their standards for the audit of internal control over financial reporting is [here](#).

9.2.2 COSO

This organisation published a framework for internal control which is not available on the web. There is a [briefing paper](#) (look under 'Publications').

9.3 Official standard setting organisations UK

9.3.1 Financial Reporting Council

The London Stock Exchange Combined Code, which includes the Turnbull and Smith guidance notes can be downloaded from the [Financial Reporting Council website](#).

These two reports are important in relation to the duties of non-executive directors and internal audit.

[Turnbull Guidelines \(2005\)](#)

On the DTI site: The Higgs Report on, ['Review of the role and effectiveness of non-executive directors'](#)

9.3.2 UK government

The [Treasury](#) website has issued:

[Internal audit standards](#)

[Management of risk – principles and concepts \(Known as the 'Orange book'\)](#)

9.4 Risk management

9.4.1 The Association of Insurance and Risk Managers (AIRMIC)

This [site](#) has a free newsletter.

9.4.2 The Institute of Risk Management

The ['Risk Management Standard'](#) can be downloaded from this site

9.4.3 Australia and New Zealand standards

They published one of the first reports on risk management (AS/NZS 4360:1999) which has now been updated. It's not available on the net, but can be purchased. Search for 'Risk Management'.

9.4.4 Risk Management information

Matthew Leitch has written three interesting sites around internal control and risk:

[Managed Luck](#) – which provides practical methods for managing uncertainty at work

RBIA – Useful information

[Internal Controls Design](#) – which provides new ideas for internal control and risk management

[Dynamic management for an uncertain world](#) – a discussion and ideas site

9.5 Other sites

9.5.1 PricewaterhouseCoopers

[Ten imperatives for a post-Enron world](#)

9.5.2 Ernst and Young

[2001 Risk Management guide](#) (takes time to download)

[Boards need to improve their risk IQ](#)

9.5.3 Deloitte

Have a useful booklet on [internal audit in the SOX era](#)

9.5.4 Working Council for Chief Financial Officers

This [site](#) has articles on internal audit. You will need to register, but it is free.

9.5.5 American Society for Quality (ASQ)

ASQ (www.asq.org) has some articles on [Sarbanes-Oxley](#).

9.5.6 US Corporate Governance

The Conference Board Commission on Public Trust and Private Enterprise was formed in the U.S. to address widespread abuses which led to corporate scandals and declining public trust in companies, their leaders and America's capital markets. It has published a report on, [‘Corporate governance, accounting and auditing’](#).

9.6 Sites with internal audit links

[AuditNet](#)® An extensive site with many resources for internal auditors

[Internal Audit Scotland](#) Check out the briefing notes and extensive links

[Will Yancies’](#) site has good links

9.7 Sites offering software and/or consultancy

The following sites offer software, and consultancy, for implementing risk-based auditing. (No endorsement is implied).

9.7.1 Software and consultancy:

My excel database is very rudimentary. If you require a more sophisticated product for managing risks and controls, take a look at the following plus other, similar, software on the market.

[Paisley Consulting](#)

[Methodware](#)

[Magique](#)

[Risk Governance](#)

There are many software solutions, some based on Lotus Notes or Microsoft Access databases. My experience is to look at the reports they can produce and make sure you are happy with them, or can amend them easily.

9.7.2 Consultancy

[Mc² Management Consulting.](#)

This is the site of David McNamee, one of the pioneers of risk-based auditing. In 1997, he published a book, 'Risk-based auditing', most of which is still relevant. Part of the structure of my audit database is the same as a table that he suggested for audit testing, so I must have got something right! David has written books and articles, which are also available on CD. Details are on his site.

[Business Risk Management Ltd.](#)

[GEB Solutions](#)

[Wayside Network](#)

9.8 Books

Internal Audit Service, Caroline Bell, Sarah Blackburn and Andrew Chambers, published for the ICAEW by [CCH](#), ISBN 1 85355 952 0, £250. This is a loose leaf manual covering all aspects of internal auditing from Corporate Governance to managing the audit department.

Managing Risk and Achieving Turnbull Compliance, Sarah Blackburn, Accountants Digest 417, [CCH](#), ISBN 1 84140 041 6, £75.

Risk based auditing, Phil Griffiths (no relation), [link](#)

The non-designers design book (2nd edition), Robin Williams, [Peachpit Press](#), ISBN 0321193857, \$19.99. Not an internal audit book but one which is very important when much of our final product is 'written' – even if this is a 'Word' document, 'PowerPoint' presentation, or web page. Do the reports from your department *look* boring? Then get reading.

9.9 You want to manage information?

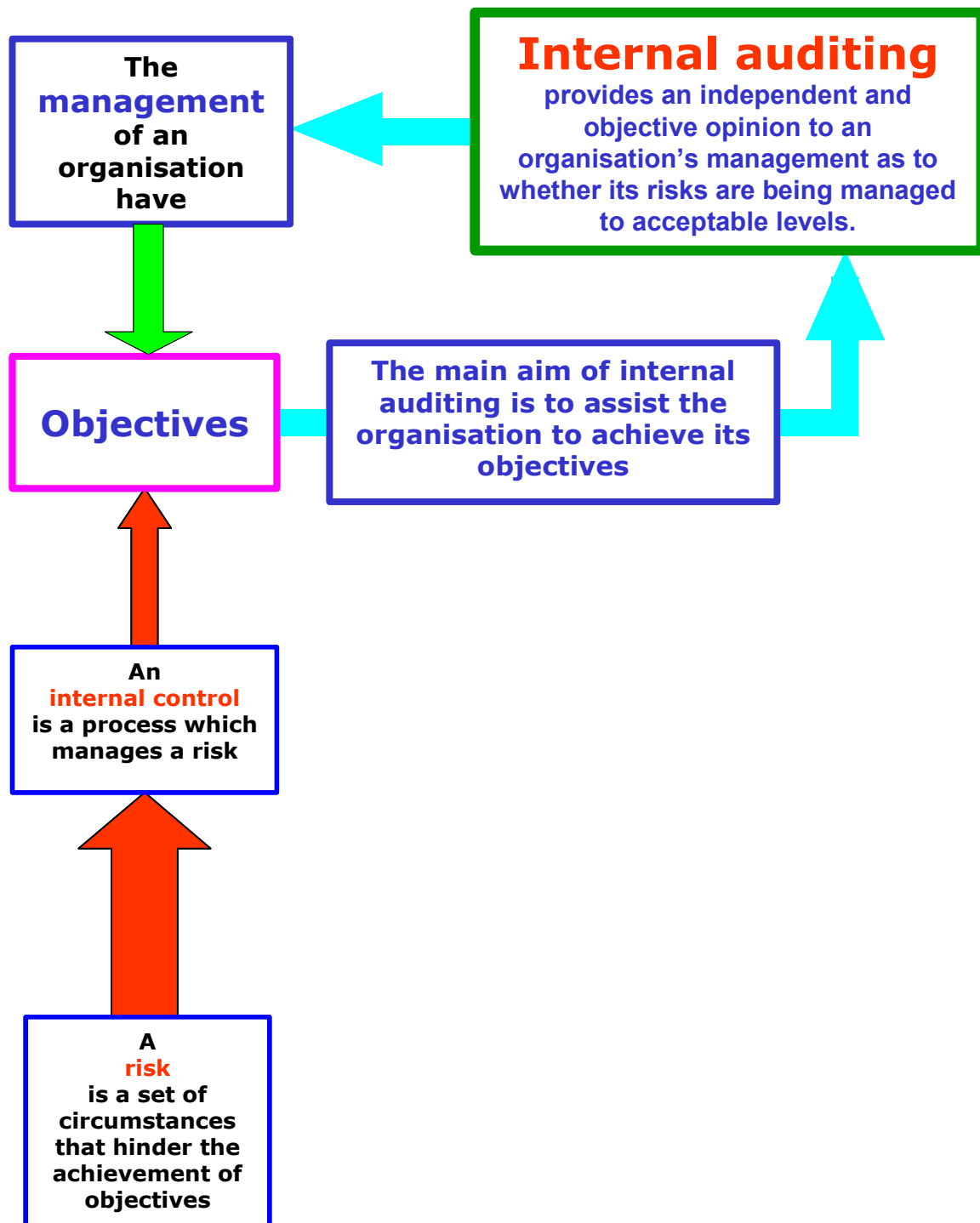
You might like to look at my other site, which considers the management of information (www.managing-information.org.uk)

10 Appendices

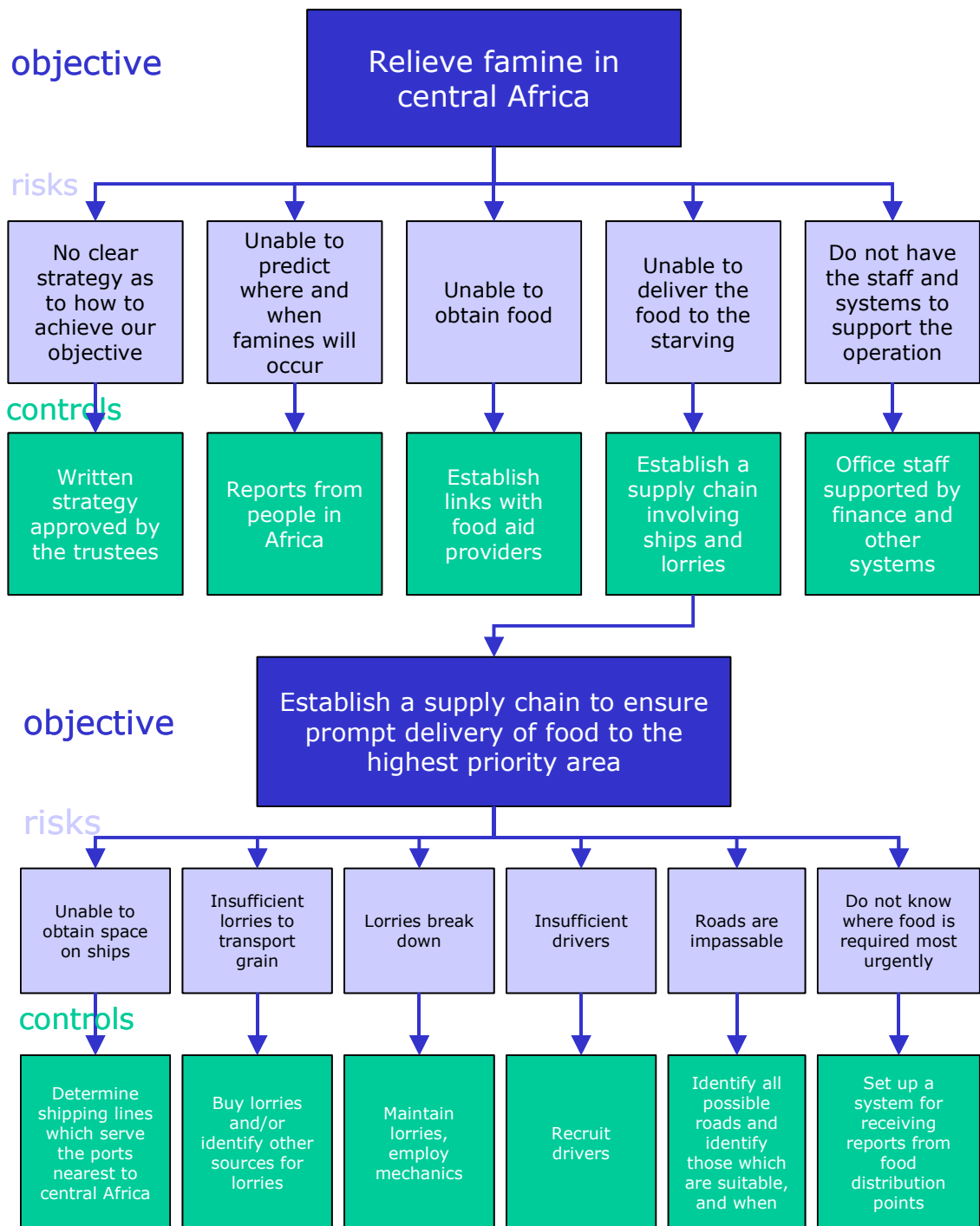
<i>Internal auditing objectives</i>	A
<i>Processes, risks and controls</i>	B
<i>Process map</i>	C
<i>Interviewing tips</i>	D
<i>Risk workshop tips</i>	E
<i>The risk register</i>	F
<i>Risk and Audit Universe – Audit planning</i>	G
<i>Risk and Audit Universe – Audit plan 2006</i>	H
<i>Quarterly plan</i>	I
<i>Summary of the individual audit process</i>	J
<i>Audit risk database</i>	K
<i>Risks to be considered</i>	L
<i>Process, risks and controls report</i>	M

Excel and PowerPoint appendices may be downloaded from
http://www.internalaudit.biz/supporting_pages/download.htm

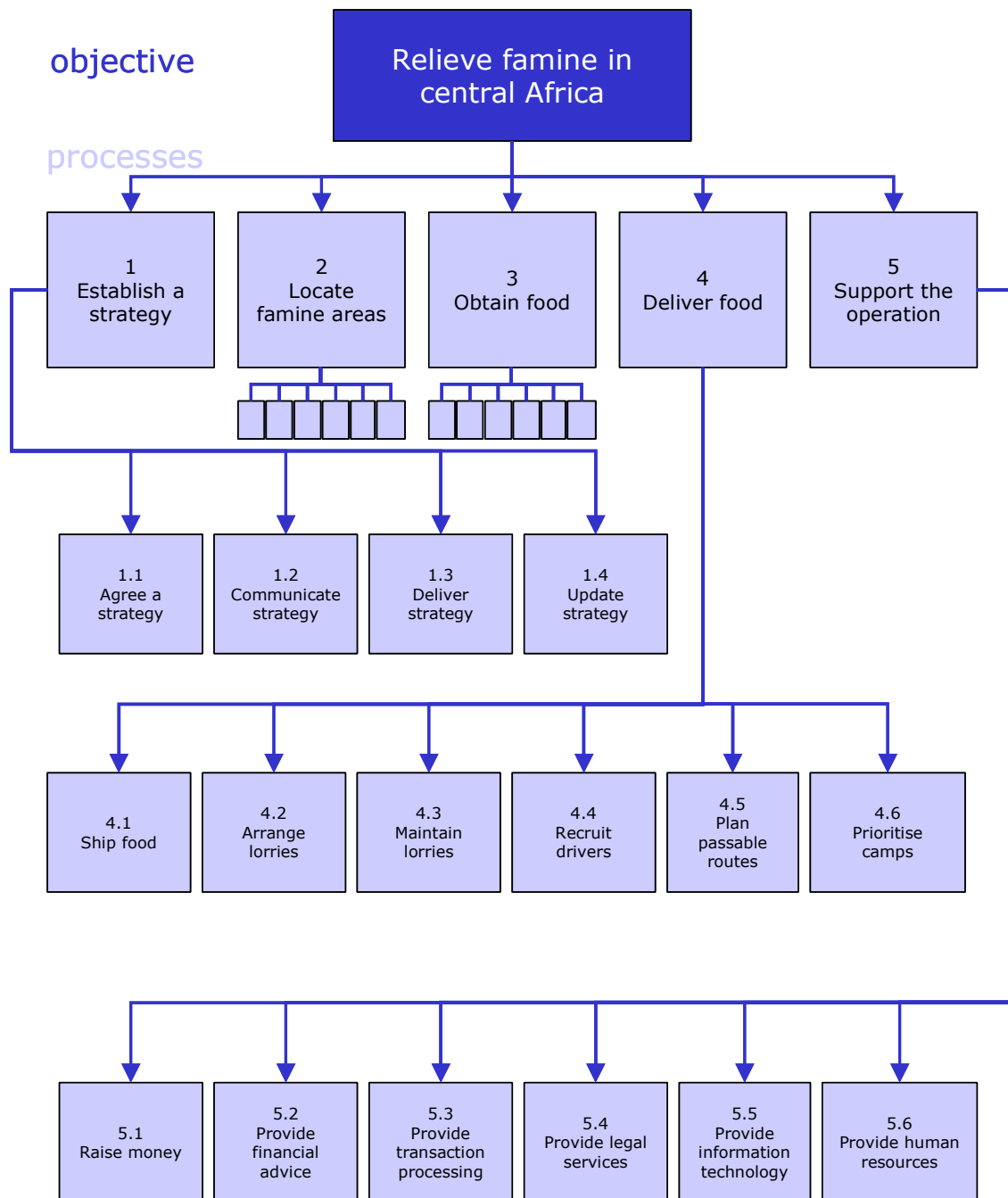
Internal auditing objectives



Processes, risks and internal controls



Process map



Interviewing

Tips are:

- Find a 'champion' for risk assessment among the group of people you are to interview. This is typically the finance director (chief financial officer). Discuss the best approach with them and get them to sell risk assessment to any doubters.
- Do your homework. Ensure you know the organisation's objectives and any specific targets the director (or equivalent) may have. Think about the risks yourself – you may have to provide examples. Talk to other parts of the business who have regular contact with the directors, to get their advice.
- Have someone to take notes, while you question. This doesn't inhibit the conversation, provided you tell the person being interviewed what is happening. You can then classify these notes and discuss them at the later risk workshop. The advantage of this approach is that it limits the possible wide ranging discussion about risks at the workshop and enables you to concentrate on the necessary action to take on the major risks. However, limiting the discussion could be a disadvantage.
- At the start of the interview explain what a risk is, and why it's important to determine them. Focus on the output of the exercise (it will help deliver the objectives), so people can see, at the start, that their time in the meeting will have benefits.
- Interview people individually, with an agenda circulated before.
- Allow an open discussion, don't try and direct it.
- Bear in mind that one of the biggest risks to any organisation is the directors, and the decisions they make. There are plenty of examples over the past few years to illustrate this point! You should therefore expect to have 'Make poor decisions' as at least one risk.
- When you have determined the risks from the interviews, these should be documented and circulated. They can be used as the basis for a risk workshop to decide on the significance of the risks, who is to ensure they are mitigated, and when by.

Running a risk workshop

In giving the detail below, I have omitted the essential points of running any meeting, such as preparing the room in advance, having a 'warm-up' session and rehearsing presentations.

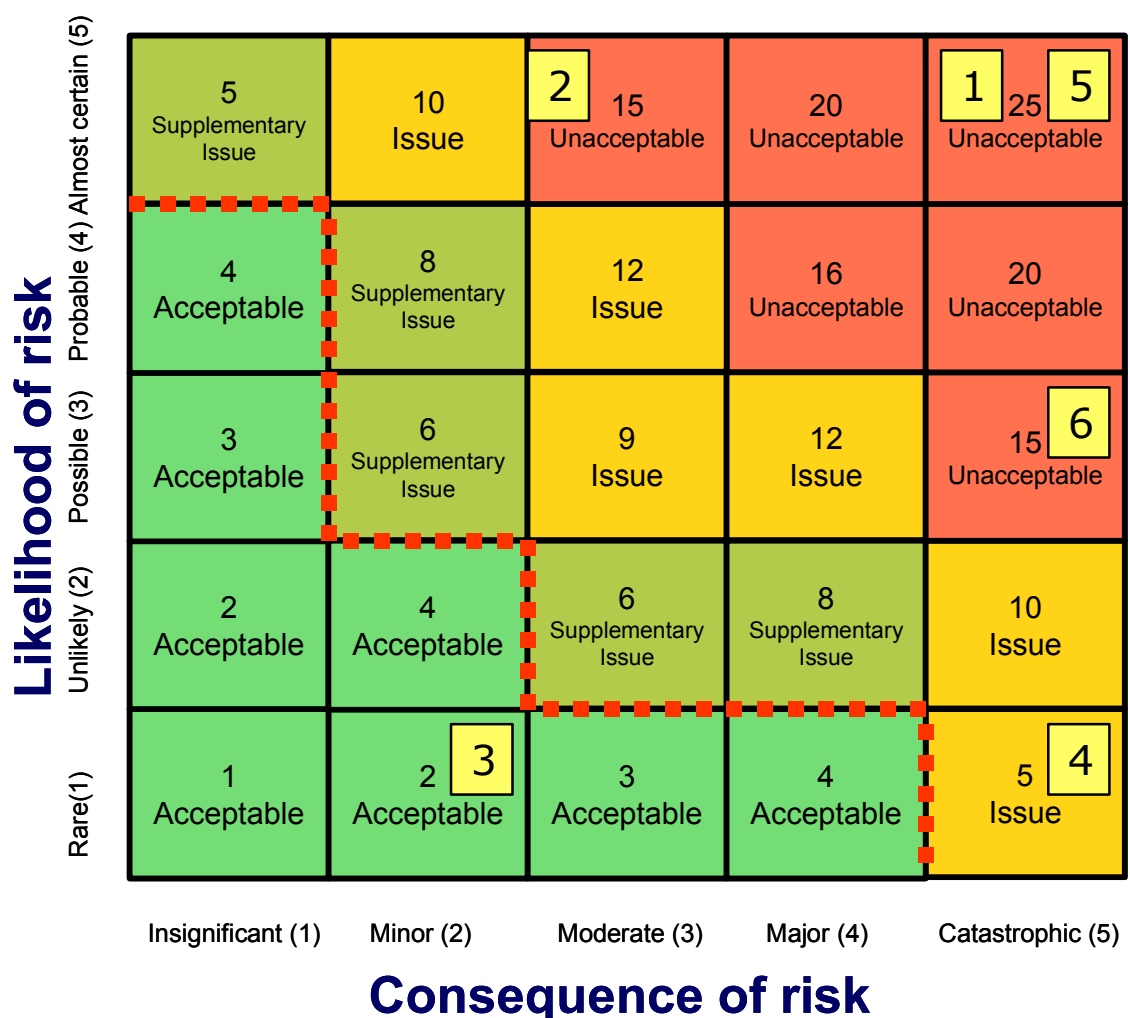
Preparation:

- Identify the people who can best identify the risks. In the case of high-level risks this will be the board (or equivalent). Avoid numbers of people more than 10. Have two meetings if necessary.
- Invite them to the workshop. Send an agenda, explaining why the output from the workshop is important.
- Experience has shown the workshop will last two hours to identify risks and their consequence and likelihood. After two hours everyone will be too tired to carry on. If you want a meeting to assign actions to risks, set up another meeting.
- If you have difficulty in getting everyone together try:
 - Adding the workshop onto a meeting that most of your people attend (for example, board meetings)
 - Have a long lunchtime workshop with a working buffet.
- Prepare an introduction, which will define a risk and illustrate the output from the meeting, and how it will be used.
- Make sure you understand the objectives that are threatened by the risks you are hoping to find.

The workshop

- You will need a chairman, to ensure that everyone gets a chance to say something and a 'scribe', to write down the risks. The role of the scribe is very important, it is not a silent role - they will ask for clarification before writing down a risk.
- Don't use complex technology as it may slow down the meeting and hence stifle lively debate. When people are shouting out risks you need a good supply of pens and flipchart paper (or chalk/white board).
- Start by giving a short (no longer than 10 minutes) presentation that you prepared earlier. This is when you can use technology.
- Ascertain, from people at the meeting, the objectives of the organisation, project or area being audited. I believe this stage to be essential, as without objectives, how can you begin to talk about risks? If people don't know their objectives, you have just found a significant risk!
- You should have no more than 6 objectives. Any more will result in people being uncertain as to priorities (another risk). These objectives should be those of the organisation, project, or area being audited, not your objectives!
- Write each objective on the top of a flip chart page, or whatever you are using to record the risks. They must be visible to the entire meeting.

- For each objective, ask members of the team to shout out the risks which might hinder the achievement of this objective. The scribe writes them down for all to see, giving each a unique number. This is where the scribe is important, as he, or she, will ask for clarification if a risk is not understood by all. Don't worry if one risk affects more than one objective, or you can't easily allocate a risk to an objective, the important task is to record the risk once against any relevant objective. This risk identification takes about an hour.
- You should now have individually numbered risks noted on flip charts or similar. The next stage is to get the meeting to agree how likely these are to occur and what their consequence will be if they do occur.
- Draw two axes on a large piece of paper (I use four flip chart sheets stuck together) and label them as below. If you are really sophisticated you can have a large laminated sheet set up, with the most significant risks highlighted in red (see below).



- For each risk, ask the meeting where it fits on the graph. This can be done by writing the number on a 'Post-it' note and sticking on the paper. The advantage of this method is that you can change your mind easily. Whatever you do, write the agreed numbers directly on the paper, as the post-it notes fall off when you take it down!

We have defined likelihood and consequences measures for a 5X5 grid but you may wish to make up your own, particularly assigning monetary values to 'consequence'

- So you now know what risks are threatening your objectives, and which ones are considered significant. Experience shows that you also have a group of people who now understand, if they didn't before, the importance of understanding risks.
- You will have taken about two hours to reach this point and everyone is exhausted. STOP NOW!

Assigning risks

- The next stage is to consider how each risk is being, or should be mitigated, by internal controls, who should be accountable and when they should have completed their task.
- This can be done using another meeting of all the people involved, an individual meeting, for example with the project sponsor, or several meetings, for example if you are wanting to determine the internal controls present as part of an audit.

The risk register (part only) – inherent scores

Level 1 process	Level 2 process	Process Description	Risk	Consequence of risk	Risk source	Inherent risks		
						Cons.	Like.	Sig.
Establish a strategy	Agree a strategy	The trustee's of the charity define the future aims and plans	Management team do not unanimously support it	Strategy not actioned with the result that it does not achieve its aims	Risk workshop with directors 15-Dec-2005	5	5	25
Establish a strategy	Agree a strategy	The trustee's of the charity define the future aims and plans	Strategy might not be the best to achieve our objectives	Charities aims not achieved effectively and efficiently. Possible loss of funds	Risk workshop with directors 15-Dec-2006	5	5	25
Establish a strategy	Communicate strategy	Tell all staff about the strategy and its importance to them	People in the organisation are unaware of the strategy	Charities aims not achieved effectively and efficiently. Possible loss of funds	Risk workshop with directors 15-Dec-2005	5	5	25
Establish a strategy	Deliver strategy	The strategy is converted into targets and action for all staff	Strategy not converted into action	Charity does not achieve its objectives	Risk workshop with directors 15-Dec-2005	5	5	25
Establish a strategy	Deliver strategy	The strategy is converted into targets and action for all staff	People in the organisation do not have personal targets linked delivering the strategy	Charity does not achieve its objectives. Loss of morale, staff leave	Risk workshop with directors 15-Dec-2005	5	5	25
Establish a strategy	Deliver strategy	The strategy is converted into targets and action for all staff	New projects do not add value	Loss of funds	Risk workshop with directors 15-Dec-2005	5	5	25
Establish a strategy	Update strategy	Aims and plans regularly updated	Strategy not updated to take account of changing circumstances	Charity does not achieve its objectives	Risk workshop with directors 15-Dec-2005	5	5	25
Locate famine areas	Monitor rainfall	Receive weather reports and assess their long term impact	Reliable rainfall figures for Central Africa are unavailable	Do not foresee the effects of drought	Risk workshop with Aid directors and her staff 10-Jan-2006	4	2	8
Locate famine areas	Monitor planting	Understand how much planting has been carried out	Information on successful planting for next year's harvest is not available	Do not anticipate food shortage	Risk workshop with Aid director and her staff 10-Jan-2006	3	3	9
Locate famine areas	Monitor crop forecasts	Understand what harvest is likely to be, using weather and planting reports	Information predicting next year's harvest is not available	Do not anticipate food shortage	Risk workshop with Aid director and her staff 10-Jan-2006	3	3	9

Risk and audit universe – planning (part)

As at 3 April 2006

Process Description	Risk	Consequence of risk	Inherent risks			Last Audit	Adjusted inherent score			Process owner	Audit Group	
			Cons.	Like.	Sig.		Opinion	Year	Gap			Factor
The trustee's of the charity define the future aims and plans	Management team do not unanimously support it	Strategy not actioned with the result that it does not achieve its aims	5	5	25	green	2003	3	0.75	18.75	Chairman of Trustees	A
The trustee's of the charity define the future aims and plans	Strategy might not be the best to achieve our objectives	Charities aims not achieved effectively and efficiently. Possible loss of funds	5	5	25	amber	2005	1	0.5	12.5	Chairman of Trustees	B
Tell all staff about the strategy and its importance to them	People in the organisation are unaware of the strategy	Charities aims not achieved effectively and efficiently. Possible loss of funds	5	5	25	red	2005	1	0.75	18.75	Personnel Director	C
The strategy is converted into targets and action for all staff	Strategy not converted into action	Charity does not achieve its objectives	5	5	25	n/a	never done	n/a	1	25	Chairman of Trustees	D
The strategy is converted into targets and action for all staff	People in the organisation do not have personal targets linked delivering the strategy	Charity does not achieve its objectives. Loss of morale, staff leave	5	5	25	n/a	never done	n/a	1	25	Personnel Director	C
The strategy is converted into targets and action for all staff	New projects do not add value	Loss of funds	5	5	25	n/a	never done	n/a	1	25	Chairman of Trustees	E
Aims and plans regularly updated	Strategy not updated to take account of changing circumstances	Charity does not achieve its objectives	5	5	25	n/a	never done	n/a	0.75	18.75	Chairman of Trustees	D
Receive weather reports and assess their long term impact	Reliable rainfall figures for Central Africa are unavailable	Do not foresee the effects of drought	4	2	8	green	2004	2	0.5	4	Aid Director	F
Understand how much planting has been carried out	Information on successful planting for next year's harvest is not available	Do not anticipate food shortage	3	3	9	green	2004	2	0.5	4.5	Aid Director	F

Risk and audit universe – ongoing (part)

Risk	Process owner	Audit Group	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
Strategy not converted into action	Chairman of Trustees	D	133	Strategy roll-out	5	Q1	Smith	complete	20-Mar-06	21-Mar-06	green
Strategy not updated to take account of changing circumstances	Chairman of Trustees	D	133	Strategy roll-out		Q1	Smith	complete	20-Mar-06	21-Mar-06	green
People in the organisation are unaware of the strategy	Personnel Director	C	134	Person target setting		Q2	Khan	planned	17-Jul-06		
People in the organisation do not have personal targets linked delivering the strategy	Personnel Director	C	134	Person target setting	10	Q2	Khan	planned	17-Jul-06		
New projects do not add value	Chairman of Trustees	E	135	Project Approval	20	Q3			29-Sep-06		
Donor countries will not provide food	Aid Director	G	136	Obtaining food - donation	20	Q2	Smith	fieldwork	12-May-06		
Pay too much for the food	Aid Director	I	137	Obtaining food - purchase	25	Q2	Doe	fieldwork	25-May-06		
Do not have sufficient funds	Finance Director	I	137	Obtaining food - purchase		Q2	Doe	fieldwork	25-May-06		
Routes become impassable due to the weather	Logistics Director	L	138	Route planning	17	Q2	Doe	planned	23-Jun-06		
Routes become impassable due to bandits	Logistics Director	L	138	Route planning		Q2	Doe	planned	23-Jun-06		
Fail to plan passable routes to the camps	Logistics Director	L	138	Route planning		Q2	Doe	planned	23-Jun-06		
Do not know where camps are	Aid Director	L	138	Route planning		Q2	Doe	planned	23-Jun-06		
Do not know where the people in most need are	Aid Director	L	138	Route planning		Q2	Doe	planned	23-Jun-06		

Risk	Process owner	Audit Group	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
Current requirement for Corporate Governance are not understood	Audit Committee Chairman	Q	139	Corporate Governance	30	Q1	Khan	report	21-Apr-06		
No policy on Corporate Social Responsibility (CSR) set up	Chairman of Trustees	R	140	Corporate Social Responsibility	30	Q1	Doe	report	21-Apr-06		
Lose money through failure of high risk investments	Finance Director	S	141	Investments	20	Q2	Smith	scoping	9-Jun-06		
Loss of the Charity's assets	Various	AB	142	Security of assets	30	Q2	Khan	scoping	9-Jun-06		
Management team do not unanimously support it	Chairman of Trustees	A	143	Strategy		Q3	Smith	planned	30-Jun-06		
Do not know quantities to order	Aid Director	H	144	Forecasting	17	Q2	Doe	planned	14-Jul-06		
No ships available	Logistics Director	J	145	Transport to docks		Q1	Khan	complete	15-Feb-06	8-Mar-06	green
No suitable docking facilities near to famine area	Logistics Director	J	145	Transport to docks	30	Q1	Khan	complete	15-Feb-06	8-Mar-06	green
Do not negotiate best rates	Logistics Director	J	145	Transport to docks		Q1	Khan	complete	15-Feb-06	8-Mar-06	green
Labour to load lorries not available	Logistics Director	K	146	Transport to camps		Q1	Smith / Khan	complete	1-Mar-06	2-Mar-06	green
Lorries not available to move food inland	Logistics Director	K	146	Transport to camps	40	Q1	Smith / Khan	complete	1-Mar-06	2-Mar-06	amber
Fuel not available for lorries	Logistics Director	K	146	Transport to camps		Q1	Smith / Khan	complete	1-Mar-06	2-Mar-06	amber
Lorries break down	Logistics Director	K	146	Transport to camps		Q1	Smith / Khan	complete	1-Mar-06	2-Mar-06	green
Spares not available	Logistics Director	K	146	Transport to camps		Q1	Smith / Khan	complete	1-Mar-06	2-Mar-06	amber
Mechanics not available	Logistics Director	K	146	Transport to camps		Q1	Smith / Khan	complete	1-Mar-06	2-Mar-06	red
Drivers not available	Logistics Director	K	146	Transport to camps		Q1	Smith / Khan	complete	1-Mar-06	2-Mar-06	red

Risk	Process owner	Audit Group	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
Money may be fraudulently removed	Finance Director	Y	147	Bank and cash	20	Q3	Doe	planned	15-Sep-06		
Transactions posted to incorrect general ledger accounts	Finance Director	Z	148	General ledger	10	Q1	Doe	complete	31-Mar-06	23-Mar-06	green
Strategy might not be the best to achieve our objectives	Chairman of Trustees	B	149	Strategy re-think	20	Q2	Khan	planned	7-Jul-06		

TOTAL (days) for planned audits in 2006 339

Resource calculation

Available (3 auditors)	
Weekdays	780
Less Holidays	-90
Less Training	-15
Less Projects	-200
Less Secondments	-50
Available for audits	425
Available for other audits	86

Quarterly plan (part)

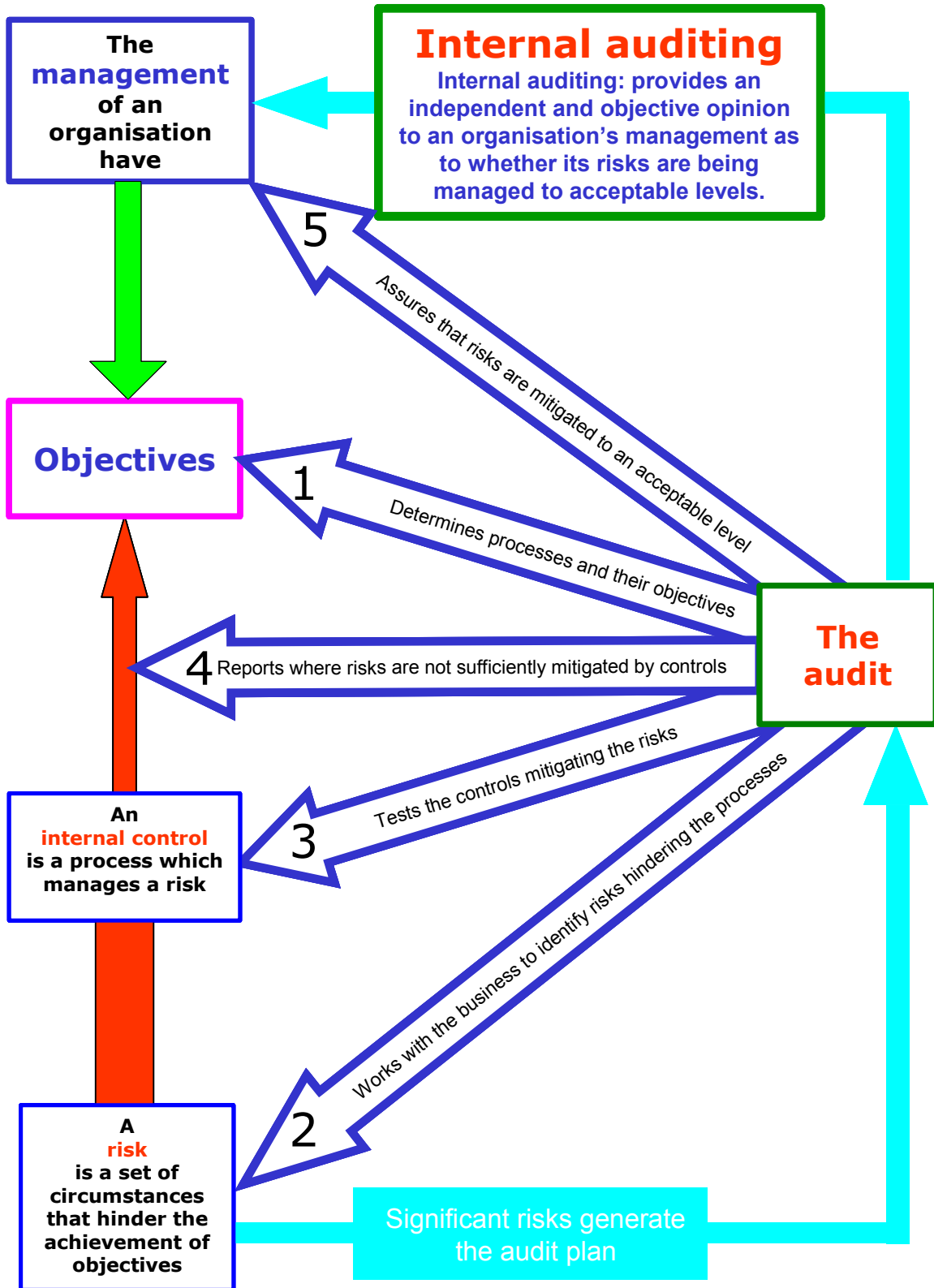
As at 3 April 2006

			Original	Planned	14	15	16	17	18	19	20	21	22	23
Name	No	Audit	Budget	now	03-Apr	10-Apr	17-Apr	24-Apr	01-May	08-May	15-May	22-May	29-May	05-Jun
Smith		Annual and Bank holidays				1	1		1				1	
Smith	136	Obtaining food - donation	20	15	4	3	3	4		1				
Smith	141	Investments	20	18	1		1	1	3	4	3	4	4	1
Smith	143	Strategy	16	21		1			1		2	1	4	4
Smith	150	SAP implementation project		7										
		Total days		65	5	5	5	5	5	5	5	5	5	5
Doe		Annual and Bank holidays		5		2	1		1				1	
Doe	140	Corporate Social Responsibility	30	5	4		1							
Doe	137	Obtaining food - purchase	25	18	1	3	2	4	4	3		1		
Doe	138	Route planning	17	17			1				1	4	4	2
Doe	144	Forecasting	17	17				1			1	1		2
Doe	147	Bank and cash	20	3										
		Total days		65	5	5	5	5	5	5	5	5	5	5
Khan		Annual and Bank holidays		8		5	1		1				1	
Khan	139	Corporate Governance	30	5	4		1							
Khan	142	Security of assets	30	27	1		2	5	4	5	5	4	4	1
Khan	149	Strategy re-think	20	16			1						1	3
Khan	134	Person target setting	10	8									1	1
Khan		Secondment to accounts		1										
		Total days		65	5	5	5	5	5	5	5	5	5	5

Key to plan

scope	fieldwork	report
-------	-----------	--------

Summary of the audit process



Audit database (146 Transport of food to camps)

Risk on register	Level 3 process	Risk for this audit	Control	Monitoring	Tests	Issue	Action	Conc	Conc	
(appendix H)								Risks	Controls	
Risks are not known		Risks are not known		None	Examine processes to set up the risk register and examine the register	No register	A risk assessment will be carried out as part of the contracting process (see below)	Red	n/a	
Significant risks are not understood		Significant risks are not understood		None	Examine the process to score the risks		As above	Red	n/a	
Significant risks are not controlled		Significant risks are not controlled		None	Check controls - below		As above	Red	n/a	
	4.2.1	Receive instructions from country office	Instructions not received	Country office confirms receipt.	HQ chases if no confirmation received	Checked all instructions and confirmations for 2003. All satisfactory	None	n/a	n/a	Green
	4.2.1	Receive instructions from country office	Instructions are late	No controls at HQ to ensure instructions are sent on time	None	n/a	No controls at HQ to ensure instructions are sent on time	Country Director to assume responsibility for notifying the country office	n/a	Amber
Drivers not available	4.2.2	Hire drivers	Drivers not available	List of drivers available for hire is kept by the compound office	None	Checked list. It is not regularly updated	Drivers may not be available	The use of contractors is to be considered	n/a	Red
	4.2.1	Hire drivers	Drivers not properly qualified	Drivers documents are checked and copies made	None	Checked copies exist.	Documents could be forged	The use of contractors is to be considered	n/a	Green
	4.2.2	Plan route	Route is blocked	Work with other agencies and the military to plan routes	None	Check the last plan. Examine dates of collection and delivery	HQ also tries to plan routes	Local office to plan routes	n/a	Green
	4.2.3	Plan route	Route is dangerous	The army escorts convoys	None	Ask drivers and supervisor about escorts	None - escorts are provided	n/a	n/a	Green
	4.2.4	Arrange to collect food	No food available!	HQ arrange for food to available in the warehouses	n/a	Check loading sheets for the lorries	None - food was available	n/a	n/a	Green

Risk on register	Level 3 process		Risk for this audit	Control	Monitoring	Tests	Issue	Action	Conc	Conc
(appendix H)									Risks	Controls
Fuel not available for lorries		Load fuel	Fuel not available for lorries	Fuel is stored in the compound	n/a	Check fuel tanks	Tanks were empty, although stock records showed they should be full	The use of contractors is to be considered	n/a	Red
Labour to load lorries not available	4.2.5	Load food	No loaders	The warehouse provides loaders	The supervisor maintains day-to-day control	Supervisor said no problem in the past	None	n/a	n/a	Green
	4.2.6	Deliver to camp	Food is stolen	Army and police provide some protection	The supervisor maintains day-to-day control	Question staff and other agencies about problem	Theft is a problem, but as well controlled as possible	No extra action possible/n/a		Amber
Lorries not available to move food inland	4.3.1	Check lorries are working	Lorries are found to be unsuitable for the journey	Lorries are serviced and tested	The supervisor maintains day-to-day control	Request a ride in the lorries	2 lorries were not working due to lack of maintenance (bad brakes)	The use of contractors is to be considered	n/a	Red
	4.3.1	Check lorries	Check is not complete	Maintenance schedules are signed by the senior mechanic	The supervisor maintains day-to-day control	Check schedules	Scheduled checks not always carried out due to a lack of mechanics	The use of contractors is to be considered	n/a	Amber
	4.3.1	Check lorries	Action is not taken on faults	Maintenance schedules are signed by the senior mechanic	The supervisor maintains day-to-day control	Check schedules	Repairs not always carried out due to a lack of mechanics	The use of contractors is to be considered	n/a	Amber
Mechanics not available	4.3.1	Check lorries	Lack of mechanics	Two mechanics are on the permanent staff	The supervisor maintains day-to-day control	Talk to mechanics. Examine work sheets	Only one, inexperienced mechanic on the staff	The use of contractors is to be considered	n/a	Red
	4.3.2	Carry out maintenance checks as per the lorry manual	Maintenance checks not carried out thoroughly	Maintenance schedules are signed by the senior mechanic	The supervisor maintains day-to-day control	Check schedules	Scheduled checks not always carried out due to a lack of mechanics	The use of contractors is to be considered	n/a	Amber
	4.3.3	Repair lorries as necessary	Repairs not satisfactory	Lorries checked by compound supervisor	The supervisor maintains day-to-day control	Request a ride in the lorries	1 Lorry was badly damaged	The use of contractors is to be considered	n/a	Amber
	4.3.3	Repair lorries as necessary	Repairs not necessary	Request for repairs and spare parts is approved by the compound supervisor	The supervisor maintains day-to-day control	Check request documents	No documents exist for requesting spares	The use of contractors is to be considered	n/a	Amber

Risk on register	Level 3 process		Risk for this audit	Control	Monitoring	Tests	Issue	Action	Conc	Conc
(appendix H)									Risks	Controls
Spares not available	4.3.3	Repair lorries as necessary	Spares not available	HQ arrange for spares to be shipped out	The supervisor maintains day-to-day control	Talk to supervisor and mechanic. Examine any available documentation	Spares can take months to arrive	The use of contractors is to be considered	n/a	Red
	6.6.1	Maintain systems	Data lost through computer failure	Not applicable. No computer on site	n/a	n/a	n/a	n/a	n/a	n/a
Staff are not competent	6.7.1	Establish job descriptions	Staff competencies required have not been identified	Job descriptions are maintained for all jobs	None	Check for job descriptions of all staff levels	No job descriptions exist.	Job descriptions will be written by the end of March 2004	n/a	Red
	6.7.2	Carry out regular appraisals	Actual competencies of the staff have not been matched with required competencies	All staff have two appraisals every year	None	Check appraisal files	No appraisals are carried out.	Targets will be set by the end of March and staff will be appraised on these by the end of September	n/a	Red
	6.7.3	Training of staff	Training is not provided	Appraisals identify training needs	None	Check appraisal files	Mechanics are not trained - but move on too quickly	The use of contractors is to be considered	n/a	Red
	6.7.3	Training of staff	Staff not allowed to attend training	None	None	Question staff who have been on courses	No courses available	We will ensure staff are trained as part of the introduction of contractors	n/a	Amber
Loss of the Charity's assets	6.8.1	Provide security	Loss of the Charity's assets	The compound is surrounded by a high fence	None	Asked staff about security	The fence is regularly broken down - hence the fuel has been stolen	The use of contractors is to be considered	n/a	Amber

This is only part of the audit database. It should be downloaded from http://www.internalaudit.biz/supporting_pages/download_manual.htm

Risks to be considered

The following key risks should be considered in any audit although, in practice, they may be more specific, and extensive, depending on the audit area.

Risk	Possible controls
Risk management	
Risks are not being managed	Risks workshops to determine risks, allocate owners, determine controls and how their operation is monitored
Fraud	
Assets could be removed from the company	Physical controls (for example a safe)
	Preventive controls (for example division of duties, authorisation levels, passwords)
	Detection controls exist (tagging of goods, reconciliations, stock counts)
Competencies	
Staff competencies required have not been identified	Job descriptions for all staff, showing competencies required
Actual competencies of the staff have not been matched with required competencies	Regular appraisals. Linked to training
Training is not provided	Appropriate training courses available
Staff not allowed to attend training	Monitoring attendance at courses and follow up by a senior manager committed to training
Contingency	
Major 'incident' destroys important company resources	A Business Contingency Plan exists, has been tested and kept up to date
Computer	
There are many risks connected with computers. The controls over some of these, such as viruses and access to change programs, can be checked as part of audits to look specifically at the risks. Controls over other risks, such as access to change data, can be considered in the audit which involves testing this data.	

Transport of food - processes, risks and controls report

Level 3 process	Risk	Control
Risk management		
Identify risks	Risks are not known	Risks not identified
Evaluate risks	Significant risks are not understood	None
Manage risks	Significant risks are not controlled	None
Arrange land transport		
4.2.1 Receive instructions from country office	Instructions not received	Country office confirms receipt.
4.2.1 Receive instructions from country office	Instructions are late	No controls at HQ to ensure instructions are sent on time
4.2.2 Hire drivers	Drivers not available	List of drivers available for hire is kept by the compound office
4.2.1 Hire drivers	Drivers not properly qualified	Drivers documents are checked and copies made
4.2.2 Plan route	Route is blocked	Work with other agencies and the military to plan routes
4.2.3 Plan route	Route is dangerous	The army escorts convoys
4.2.4 Arrange to collect food	No food available!	HQ arrange for food to be available in the warehouses
Load fuel	Fuel not available for lorries	Fuel is stored in the compound
4.2.5 Load food	No loaders	The warehouse provides loaders
4.2.6 Deliver to camp	Food is stolen	Army and police provide some protection
Maintain lorries		
4.3.1 Check lorries are working	Lorries are found to be unsuitable for the journey	Lorries are serviced and tested
4.3.1 Check lorries	Check is not complete	Maintenance schedules are signed by the senior mechanic
4.3.1 Check lorries	Action is not taken on faults	Maintenance schedules are signed by the senior mechanic
4.3.1 Check lorries	Lack of mechanics	Two mechanics are on the permanent staff
4.3.2 Carry out maintenance checks as per the lorry manual	Maintenance checks not carried out thoroughly	Maintenance schedules are signed by the senior mechanic
4.3.3 Repair lorries as necessary	Repairs not satisfactory	Lorries checked by compound supervisor

4.3.3	Repair lorries as necessary	Repairs not necessary	Request for repairs and spare parts is approved by the compound supervisor
4.3.3	Repair lorries as necessary	Spares not available	:HQ arrange for spares to be shipped out

Provide information technology

6.6.1	Maintain systems	Data lost through computer failure	:Not applicable. No computer on site
-------	------------------	------------------------------------	--------------------------------------

Provide human resources

6.7.1	Establish job descriptions	Staff competencies required have not been identified	:Job descriptions are maintained for all jobs
6.7.2	Carry out regular appraisals	Actual competencies of the staff have not been matched with required competencies	:All staff have two appraisals every year
6.7.3	Training of staff	Training is not provided	:Appraisals identify training needs
6.7.3	Training of staff	Staff not allowed to attend training	:None

Provide security

6.8.1	Provide security	Loss of the Charity's assets	:The compound is surrounded by a high fence
-------	------------------	------------------------------	---

Provide continuity

6.9.1	Identify documents required to achieve the objective of these processes	Documents may not be recorded	:None
6.9.2	Decide on arrangements to safeguard these	Level of protection may not be sufficient	:None

Version control

Version number	Date issued	Changes made to previous version
1	16-Feb-2003	Issue of first version
1.0.1	2-Mar-2003	More links, biography. Note re IIA UK position statement on RBIA
1.0.3	9-Mar-2003	Link to draft position paper. Definition of Enterprise-wide risk management
1.1.0	13-Nov-2003	Updated notes on Combined Code, SarbOx, PCAOB. Updated links plus other minor amendments
1.1.1		Link added
1.2.0	14-May-2004	Amendments to chapter 2 and chapter 3 to make it consistent with the manual
1.2.1	1-Jul-2004	The useful information section has been re-arranged
1.2.2	26-Aug-04	Link to David McNamee site added
2.0.0	6-Oct-05	Major revision.
2.0.2	30-Jan-2006	Changes made to take account of IIA Guidance Note
2.0.3	15-Mar-06	Minor changes