Internal auditing

An introduction

David Griffiths

PhD FCA

www.internalaudit.biz

Version 6.0

Contents

David M Griffiths

Biography

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

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

I returned to be Head of the internal audit department (Chief Audit Executive) 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 reorganization of Accounting Services, I returned to internal audit, as Internal Audit Manager. 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 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. I also served as a trustee for an almshouse charity, where I compiled the risk database in Microsoft Access, which is available on the website.

The views expressed in this book and on the web site, are my own and are not endorsed by the IIA or Boots.

I have written websites on managing information (http://www.managing-information.org.uk/), Specifying, Choosing and Implementing Computer Systems (www.systemsimplementation.co.uk/) and teaching the basics of computing (www.learncomputing.org.uk).

Introduction

Welcome to risk based internal auditing (RBIA). The aim of this website, and the books and spreadsheets available from it, is to push out the boundaries of internal auditing by providing practical ideas on implementing (risk based) internal auditing. These ideas are not meant to represent 'best practice' but to be thought provoking.

There are four books with associated spreadsheets

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

I won't claim that my ideas in this book are shockingly original; indeed most are built on accepted thinking and practices. This book is not intended to be a lengthy, well-researched academic treatise, but a simple introduction. I've therefore used an informal, as opposed to an academic, style. I'll leave you to judge whether this works. I would also advise you to look for further information from the links on the website.

This book seeks to move the basis of internal auditing from 'risk based' to 'objective focused'. However, I have retained the title of 'Risk Based Internal Auditing' because it is a recognized title understood by internal auditors and used by search engines.

This introduction is aimed at anyone interested in internal auditing, from audit committee members to students. It is split into chapters. The first deals 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 organization and are more suited to readers who have some experience of internal auditing.

Two spreadsheets support this book: *rbiaintroduction.xlsx* has worksheets which provide more detail about the planning of audits; *146workingpapers.xlsx* provides example for a specific audit, including supporting documentation.

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.

Please remember when reading the book and the spreadsheets that they are only presenting *simplified* examples. In practice there would be many more objectives, risks and controls than I have listed. It is your responsibility to take the ideas you like and adapt them for your organization. Please don't blindly copy them.

I should mention that this book discusses the objectives of internal auditing as a 'tool' within an organization, and *not* the objectives of an internal audit department. Hopefully, the primary objective of an internal audit department 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 uses US spellings, since the majority of readers use this dictionary. However some of the terms used (supplier instead of vendor) will be UK based. Sorry for any confusion.

Many thanks and happy reading…

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

Acknowledgements

I'd like to acknowledge the contributions made by colleagues at Boots and Norman Marks in his blog (https://normanmarks.wordpress.com/) which have helped form the ideas in this book, although they may not necessarily agree with them.

1 The basics

1.1 What is the purpose of 'internal auditing?'

If you look at the work that internal auditors are doing throughout the world, most of it will involve 'internal controls'.

So what are 'internal controls'? They are processes which reduce risks. So, if you are a store which takes cash, you have a process of putting this cash in a safe to reduce the risk of it being stolen.

What are risks? Risks are circumstances which threaten the achievement of objectives (other definitions exist). You have an objective of making money from your store and the risk of that money being stolen threatens your objective.

Internal auditing therefore ***checks that the internal controls which reduce the risks that threaten our objectives are working properly***. That's a simple explanation which ignores opportunities so let's look at the detail, starting with objectives, then looking at the opportunities and risks which affect their achievement before considering how to manage these opportunities for maximum benefit. We can then decide how internal auditing can assess this management.

So we first need to look at objectives and risks.

1.2 Objectives

Organizations have a reason for their existence and this reason is frequently summarized in a mission statement. NASA's mission statement is, '*Drive advances in science, technology, aeronautics, and space exploration to enhance knowledge, education, innovation, economic vitality and stewardship of Earth*'. Amazon's mission statement is, '*Our vision is to be earth's most customer-centric company; to build a place where people can come to find and discover anything they might want to buy online*.'

Mission statements are implemented by objectives. In general these will be:

1. Establish objectives to deliver the mission statement.
2. Maintain the existing organization.
3. Develop the organisation.
4. Obey applicable laws and regulations.
5. Communicate the strategy to stakeholders (owners, trustees, employees, customers).
6. Support the organization to deliver the strategy (establish a board, operations departments, administration departments).

I've used the word 'strategy' in this book which I've taken to mean a combination of the Mission Statement and the objectives which are necessary to fulfil the statement.

These objectives should be divided into sub-objectives for each level of the organization down to employee. The achievement of each of these sub-objectives will be threatened by risks and benefitted by opportunities and, as we will see, this achievement of objectives then requires decisions.

1.3 Risks

My definition of a risk:

> **A risk is a set of circumstances that threaten the achievement of objectives.**

This definition recognizes the importance 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.

So we can define an opportunity as :

> **An opportunity is a set of circumstances that contribute to the achievement of objectives.**

This example provides an important lesson: objectives have opportunities which benefit their achievement and risks which threaten their achievement. The farmer has an objective of maximizing crop yield. The flooding provides an opportunity of river silt but also carries the threat of damaging stored seed not moved to higher land. Benefits and risks are a fact of life. Some managers would like to keep the benefits but remove the risks completely, but this is impossible without closing down the entire organization (which also presents risks). So in order to maximize the chances of achieving our objectives we need to manage the benefits to get the best out of them and the risks to mitigate them.

In our example the farmer might build low walls to hold back the silt and move the seed to higher ground.

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 (and opportunities providing benefits). That doesn't mean we don't launch the product; it does mean we aim to maximize the opportunities and minimize the risks to a level where the benefits we expect to get are greater than the threats we expect to endure, 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* opportunities and risks. Ideally, we should try and quantify the opportunities benefiting and the risks threatening projects, for example by using financial risk modeling. In this way the threats can be compared with the potential benefits.

1.4 Process and decision opportunities and risks

Let's go back to our example of the Nile flooding. The Curator of the museum should have gone through a risk analysis:

Objective: to keep the exhibits safe.

Risk: The Nile floods the ground floor of the museum resulting in damage to the exhibits.

Action to reduce risk: Keep those exhibits which are difficult to move on the upper floor. Set up a plan to move exhibits from the ground floor to the upper floor when a flood is predicted.

Suppose the Nile floods much more quickly than expected, with the result that we cannot move all exhibits from the ground floor before the flood is due. Plus… the essential lift has broken down. We have some decisions to make: which exhibits to move first; whether to get more people involved in the move; whether to wait until the lift is repaired.

In the first scenario (a predicable flood and working lift) the risk results from having a museum near the Nile. It's a risk which arises from the business we're in and its location. We can call this a 'process' risk (my description so no-one else will recognize it). It's predictable, doesn't change much over time (but does change) and we have the time to consider the internal controls necessary to mitigate it.

In the second scenario (an unexpected flood and broken lift), there are several options, the benefits and risks are not easily predictable and they change quickly: can I get staff who know how to handle delicate artifacts? What if the lift cannot be repaired quickly? We can call these risks 'decision' risks and we don't necessarily have the time to carefully consider the internal controls to manage them.

So how do we differentiate between process and decision risks? Both threaten the achievement of objectives.

- A process risk arises from circumstances which threaten the operation of day-to-day activities necessary for the correct operation of the organization.
- A decision risk arises from circumstances when several choices for action are available and the best (that is the best predicted outcome when opportunities are weighed against risks) have to be chosen.

Decision risks and process risks are related: Decisions are required:

- To determine what controls are required to manage process risks.
- As part of a control. For example we may have a credit control department to reduce the risk of non-payment by customers (process risk). A decision risk occurs when a customer with overdue debts tries to place an order. Do we accept the order? Under what conditions?
- When a process risk occurs. In our example the curator anticipated a flood and took action to reduce its impact. Decisions were necessary when the action anticipated was insufficient.

What about process and decision opportunities? Considering our example; the anticipated flooding is a process opportunity for the farmer and the unexpected rapid flooding is a decision opportunity (can I get help to build retaining walls, which walls should I build first?).

Why is a distinction necessary between process and decision risks? Because the resulting controls need to be audited differently - see section 1.12 for details. Process risks are managed by specific processes which reduce their threat. Thus their presence and operation can be verified ('ticked'). Every decision is different, so only generalized processes can apply, such as: information is gathered; all possible choices are evaluated; all relevant staff are involved. These can be ticked but every decision can't be checked. Yet it is decision risks which can result in the biggest gains, or losses.

Unfortunately there is a tendency among standard-setting bodies and therefore internal auditors, to concentrate only on process risks and their management, often with little regard to the objectives whose achievement they are threatening. This is somewhat inevitable as it is human nature to fear the impact of risks while ignoring missed opportunities.

So we need to stop concentrating on process risks and start concentrating on the management of all opportunities and risks in order to maximise the likelihood of achieving our objectives. We should replace 'risk management' by 'achievement of objectives management'. This management involves the establishment of objectives, determination of opportunities and risks, and the managing of these to maximise the probability of achieving our objectives.

In the next sections we will consider: the characteristics of process and decision risks; how to mitigate (manage) the impact and likelihood of process risks; how to manage decision risks; how to assess the effectiveness of this management - which is 'internal auditing'.

1.5 Characteristics of process and decision risks

In order to demonstrate the differences between process and decision risks, we can consider their characteristics:

Characteristic	Process risk	Decision risk
Occurrence	Routine processes necessary for the correct operation of the organization fail which threatens the achievement of objectives.	An event requires a choice to be made from a series of alternative scenarios
Timing	Possible to predict well in advance	Can be unpredictable
Identification	By management from their objectives	Specific identification may not be possible until the choices available are identified. Some decision risks relate to processes, such as credit control.
Management	Mainly through internal controls (see below)	By decisions, possibly at very short notice
Complexity	Can be straightforward (Cash is stolen)	Often complex with a number of inter-linked risks and decisions (see below)
Impact if management fails	From low to catastrophic	Generally higher than the corresponding process risk which has failed.
Information required	Regular information which warns if the risk is likely to occur	Specific information required to make an informed decision
Internal audit	Check to ensure sufficient controls are present and operating	Check to ensure all staff are properly trained to make decisions appropriate to their responsibilities

Let's consider another example:

Objective: To grow the company sales by 10%

Sub-objective: take over another company

Risk: we may pay too much, or fail by offering too little

Internal controls: Financial evaluation (independently checked) to provide income and cost projections; risk evaluation; evaluation of possible scenarios; formal board approval

The risk is a process risk. We can anticipate the risk and devise controls.

Suppose a competitor now outbids us. While we could reasonably predict this might happen and have broad internal controls (form a special team dedicated to quick action, consider the highest price we might pay) the competitor may be a surprise and the price they offer near our maximum. We now have decisions to make with risks that they may be wrong: how important is it to prevent the competitor taking over this company? Should we pay more to prevent the competitor acquiring the company? Are similar companies available for takeover by ourselves or the other company? We need information about the competitor. We need to test various scenarios. We made need to consider the impact on our investors. As internal auditors we can't set up tests to check the management of these risks, all we can do is make sure that the people making the decisions are capable and properly trained, and that the information they might require is correct and available.

1.6 How do we manage process opportunities and risks?

The four accepted methods for managing risks are: terminate; transfer; tolerate; treat. We can also apply these to opportunities:

Management	Opportunity	Risk
Seize an opportunity or avoid (**terminate**) a risk	Look for opportunities, such as new products, which increase the chances of achieving objectives. May give rise to risks.	**Avoid the risks**, for example by not starting up a business selling innovative products or by closing a factory making dangerous chemicals. This may mean giving up significant opportunities.
Transfer the opportunity or risk	The organization may identify an opportunity which is too big for it to pursue. It could sell the idea on.	**Transfer** them, the best example being insurance.
Tolerate (accept) the opportunity or risk	Hot weather for an ice cream maker is an example. It could just be accepted without attempting to capitalize on the opportunity. It would be better to maximize the opportunity by increasing production (below)	**Tolerate them.** Where the cost of avoiding the risk is greater than the likely cost should the risk occur
Apply processes (**treatment)** to maximize opportunities and minimize risks	Introduce processes to maximize opportunities. For example, base the production of ice cream on weather forecasts.	Introduce some processes to **reduce the consequence or likelihood** of a risk. These processes are usually referred to as 'internal controls' and include everything from having a clear strategy to installing a fire alarm.

.

1.7 How do we manage decision opportunities and risks?

The four accepted methods for managing risks are: terminate; transfer; tolerate; treat. We can also apply these to opportunities:

Management	Opportunity	Risk
Seize an opportunity or avoid (**terminate**) a risk	If an opportunity suddenly presents itself, act quickly to maximize the benefits	**Terminate** the risk (for example close the leaking oil well)
Transfer the opportunity or risk	The organization may identify an opportunity which is too big for it to pursue. It could sell the idea on.	Not usually possible but help at handling public relations, for example, could be obtained
Tolerate (accept) the opportunity or risk	Don't seize an unexpected opportunity.	**Tolerate them.** 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.
Apply processes (**treatment)** to maximize opportunities and minimize risks	Check that all information which might be needed is easily available. Ensure staff are trained in decision making and are encouraged to identify opportunities	Anticipate various scenarios (takeover bid, CEO says something embarrassing) and plan for these by considering the options available

1.8 Internal controls

There's an important point about controls: *controls are a response to opportunity or risk*. If there is no opportunity or risk, then you don't need a control. In other words, controls are a product of an organization's need to achieve objectives.

I define any response which manages an opportunity or risk in one of the above ways as an 'internal control'. Thus:

Internal controls are processes which manage opportunities and risks in order to improve the chances of achieving objectives

1.9 Who is responsible for implementing internal controls?

The *management* of an organization is responsible for:

- Specifying the objectives of the organization and communicating them.
- Identifying the opportunities which benefit and the risks which threaten the achievement of these objectives.
- Scoring these opportunities and risks (inherent risk score).

- Establishing internal controls to manage opportunities and risks, and scoring the controlled opportunity/risk (residual risk score). This includes ensuring controls exist to maximize the benefits from decision making.
- Receiving from the controlling board their risk appetite, in terms of the scoring used.
- Informing the board about those residual risks which are still above the risk appetite (usually those which are to be tolerated).
- Assuring the organization's board that it maximizing the chances of achieving the organization's objectives by monitoring the internal controls which maximize the available opportunities and bring risks to below their risk appetite.

Management has these responsibilities because they are in the best position to know the opportunities benefiting and risks threatening their objectives, take action to implement the appropriate internal controls and monitor their continued operation.

The determination of risks across the whole organization is known as 'Enterprise-wide Risk Management', although in some organizations this may not be taken to include opportunity management or decision risks. Hence I try and avoid using the term.

1.10 How do we assess internal controls managing risks?

So, our *objectives* are benefited by *opportunities* and threatened by *risks*, which require *internal controls* to manage them. Now, if you are a manager (director, trustee, CEO, for example) you will probably want an opinion on how effective the internal controls are which manage the opportunities and risks which benefit and hinder the achievement of your objectives. You may be required to do this by law.

How do we know if an internal control is effective? What do we mean by effective?

An effective internal control is one which manages the risk down to a level which our controlling board of management (Board of Directors, Trustees, or Governors) considers acceptable. Since there are many risks within an organization we need:

- A means of measuring the significance of a risk.
- A statement from the controlling board as to which risks they consider significant and which must therefore be managed, using the measuring system we have implemented - known as their *risk appetite*.

We'll consider the detail of measuring risks and setting a risk appetite when we look at establishing an internal control framework. We will measure our risks before applying an internal control (the *inherent* or *gross* risk score) and after an internal control (*residual* or *net* risk score). We would expect our internal control to reduce the inherent risk score to a residual risk score which is less than the score our board has set as their risk appetite (*target* score).

There is much controversy in the risk management community about ‘risk appetite’. Can it be clearly defined or does it even exist? An unacceptable risk is like an elephant - difficult to describe but you know one when you see one. Most living creatures understand the difference between an unacceptable risk and an acceptable risk. Those that don't tend to be eaten. So I believe that a risk appetite exists whenever a risk exists, even if it is not possible to accurately define it in financial, or any other, terms.

1.11 How do we assess internal controls which manage opportunities?

The emphasis on risk management by statutory bodies (COSO, Finance Reporting Council and King Report to give examples in the US, UK and South Africa) has resulted in little consideration as to how to ensure opportunities are seized.

One method is to make the opportunity a risk. So the opportunity to increase profits by launching a new product becomes the risk of how much profit we might lose if we don't launch a new product. Not very satisfactory.

We can use the same method as for risks:

- Determine the opportunities helping us to achieve our objectives
- Decide on a means to measure them
- On this scale of measurement, decide at which point they deserve attention.

1.12 How do we assess decision-making controls?

I suspect most businesses lose money not through fraud, IT systems failure or even Covid-19 but through poor decision making. Therefore tests involving decision making must be part of every audit. They are included in appendix K.

Since the controls are so important, it's worth considering them at this point.

From an auditing perspective there are two types of decisions:

- Verifiable. These are usually significant decisions with an approval process involving documents which are signed off, for example by the board. Since this is a 'process' we can audit it by verifying the documents used and would expect to find
    - Rules, approved by the board, as to who can authorise what
    - The objective to be achieved by making the decision
    - The options available for achieving the objectives
    - The advantages and disadvantages of each option - costed if possible. This to include identification of all possible scenarios which might result from each option, together with any action which might be necessary. This process should highlight the opportunities and risks of each option. Where appropriate, financial modelling should be used (e.g. @RISK)
    - All staff who can contribute to the decision are involved.
    - An independent check of the financial case.
    - Information used to justify the option chosen is complete and accurate.
    - The reasons for the choosing the preferred option.
    - The actions required, by whom, to implement the option chosen.
    - Timing for implementing the option including, if appropriate, when financial outlay will occur.
    - Targets, or other means, of checking the progress of the actions required.
    - The decision required from the authoriser(s), such as the board or a senior manager.

- Non-verifiable. These are decisions made by all levels of staff every minute. They include a doctor deciding whether to operate on a patient, a museum creator deciding which exhibits to save from a Nile flood, a store worker giving a customer a refund for returned goods, or a police officer deciding whether to shoot,. As we have seen in previous sections, these are not managed by specific ('tickable') internal controls. Although there may be evidence of a decision having been taken (a report from a doctor on the operation) there may be no record of the options available (operate/don't operate) and why the option was chosen. The adequacy of non-verifiable decisions is done by checking:
  - What evidence exists that staff;
    - Know their personal objectives and how these relate to the organization's objectives?
    - Know what decisions they are permitted to take and what must be transferred to more senior staff?
    - Know what rules restrict their action?
    - Are encouraged to take decisions which seize opportunities as well as those which control risks?
    - Have been trained in the processes of decision making?
    - Have been provided with the tools which assist decision making?
    - Are provided with the information needed to make decisions?
  - What evidence exists to judge effective decision making? For example: have investment decisions achieved their expected benefits; are bad debts higher than desirable? (But note that a very low level of bad debts may indicate poor decisions which reject too many orders).

There are three possible methods for auditing controls around decision-making

1. A specific audit of decision-making processes. This is suitable for board approvals and other major decisions where the processes used should have been clearly defined (see above) and apply throughout the organization.
2. Checks as part of normal audit procedures, for example the auditing of customer refunds or new customer accounts.
3. Specific checks as part of every audit, as noted in the bullet points above and appendix K.

In the example audit (opens an Excel file) I have included a test using method 3 but not the other two.

1.13 What is the role of internal audit?

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

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

So if the organization'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 organization.

There is an assumption, hopefully justified, that the objectives of any organization 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 organization. The achievement of these objectives is benefited by opportunities and threatened by risks which should be managed below the risk appetite by internal controls. But are they? It's the role of internal audit to provide an opinion. Hence my definition:

> **Internal auditing provides an independent and rational opinion to an organization as to whether it is likely to achieve its objectives, based on the management of opportunities and risks.**

Let's look at this definition in detail:

Independent: the function carrying out the internal auditing activity is 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. It will not change any correct opinion as a result of undue pressure.

Rational: Opinions are 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 opportunities and risks are being managed in order to maximize the likelihood that objectives will be achieved. 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.

Organization: A group of people, with supporting assets, that is 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 organization will normally have to prepare financial, and other, statements for these 'stakeholders'.

Its objectives: the objectives set by the stakeholders and the sub-objectives set for every level of staff consistent with their responsibilities.

likely to achieve its objectives based on the management: Internal controls manage opportunities and risks in order to maximize the benefits from opportunities and minimize the threats from risks. Internal audit staff examine the effectiveness of internal controls in order to reach an opinion as to whether these controls are sufficient to manage the opportunities and risks and therefore ensure the likely achievement of objectives.

Opportunities and risks: The opportunities which benefit, and the risks which threaten, the achievement of the objectives specified by the stakeholders.

We could call this definition of internal auditing 'objective focussed internal auditing', but let's keep life simple and stick with 'risk based internal auditing'. If internal auditing is focussed on risks, it should be focussed on the objectives threatened by them. (This definition differs from that in the first five versions of the book. The previous definition had greater emphasis on the risks)

1.14 Where does 'risk management' fit in?

'Risk management' is a term widely used, and 'Risk Manager' jobs exist in organizations. 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 organization to identify its risks, running risk workshops, coaching staff in risk management and setting 'best practice standards'.

The Internal Audit department may be asked to provide advice, and more, on risk management.

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 IIA publication *The Role of Internal Audit in Enterprise-wide Risk Management* has further information.
- 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 organization. Ideally both functions should report to different senior managers or directors to reinforce the distinction.

1.15 Opportunities, risks: process and decision

I've discussed the need to consider opportunities as well as risks, and proposed two types of risk (process and decision) characterized by their different internal audit approach. For the rest of this book, I will usually only refer to risks, with the understanding that I am referring to both types of risk and including opportunities.

1.16 Summary

So my current definitions may be summarized:

- Opportunities benefit and risks threaten the achievement of objectives.
- Internal controls manage opportunities and risks in order to maximize the likelihood and impact of achieving objectives
- Internal auditing provides opinions about whether objectives are being, or are likely to be achieved, based on the effectiveness of internal controls.

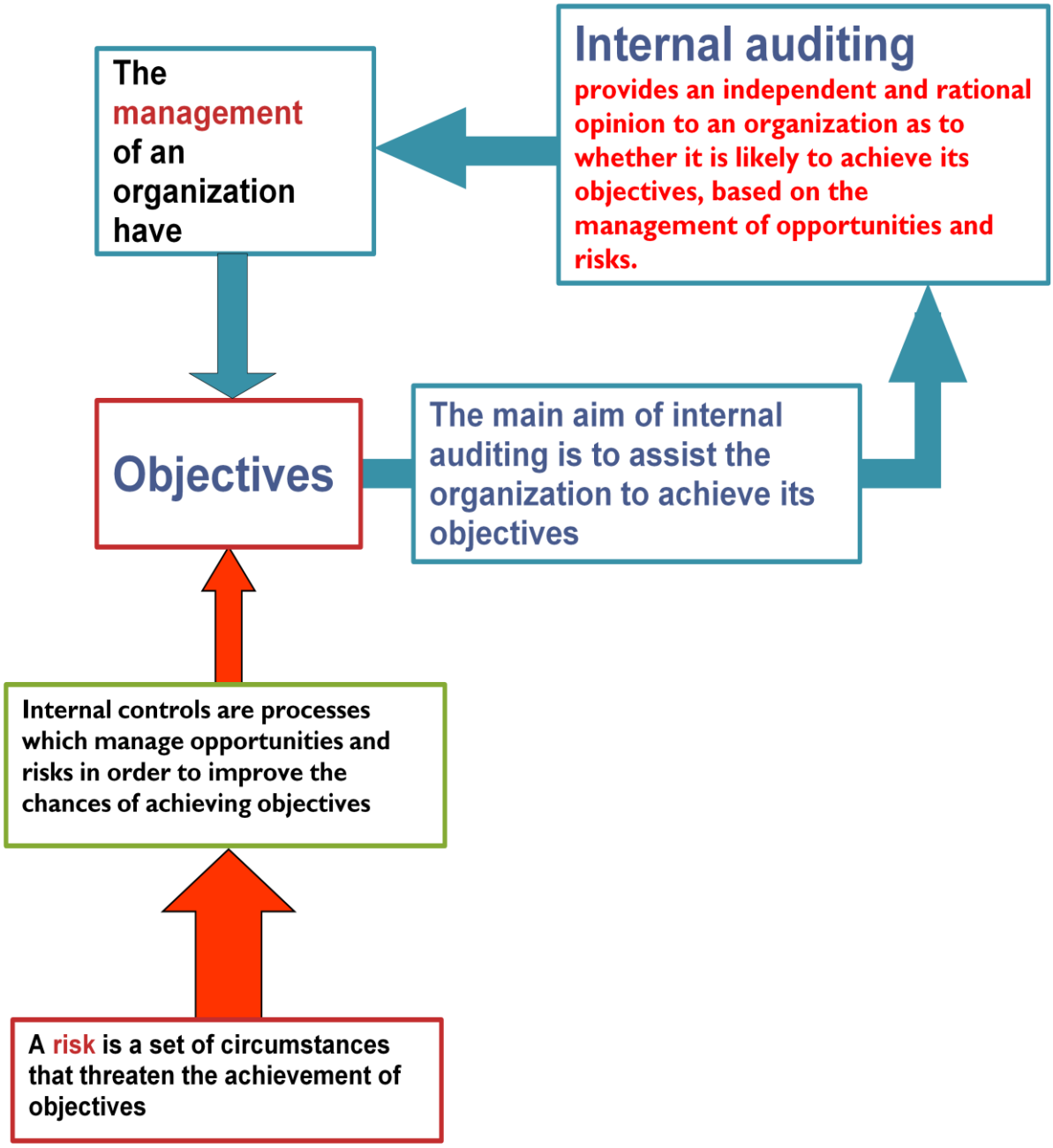
Although my definitions are not the same as those from official bodies, I prefer them because:

- They are simple
- They provide a clear trail from an organization's objectives to all the internal controls it requires, and to the purpose of internal auditing.

These definitions lead to important conclusions:

- To know which internal controls are necessary, you must know the opportunities and risks of your organization.
- To know the opportunities and risks of your organization, you must know its objectives.

This diagram summarizes the elements of internal auditing.


Internal auditing
provides an independent and rational opinion to an organization as to whether it is likely to achieve its objectives, based on the management of opportunities and risks.
The management of an organization have
Objectives
The main aim of internal auditing is to assist the organization to achieve its objectives
Internal controls are processes which manage opportunities and risks in order to improve the chances of achieving objectives
A risk is a set of circumstances that threaten the achievement of objectives

2 The internal audit opinion

2.1 What is the opinion?

If internal audit has to provide an opinion to 'the organization'.

- Who actually receives the opinion?
- What is the format of the opinion they receive?

These two questions are inter-linked because the recipients of the opinion will influence the format.

The recipients (the 'management') will include:

- Managers responsible for delivering the objectives, threatened by the risks which are managed by the controls whose operation is checked by internal audit.
- Senior managers responsible for these managers
- The board and audit committee (who may only receive summaries of opinions).

So what do these recipients require from the opinion? The board and audit committee may have to make public declarations about risk management and it is these declarations which should determine the internal audit opinion.

2.2 Declarations about the state of internal control

2.2.1 Committee of Sponsoring Organizations of the Treadway Commission (COSO) (US)

This Committee has issued an update to a document 'Internal Control - Integrated Framework' which sets out requirements for establishing internal controls in an organization. This document includes templates to assist in forming an opinion about the state of internal controls. The summary template (Overall Assessment of Internal Control) has as its final question:

'Is the overall system of internal control effective? <Y/N>*' (* If it is determined that there is a major deficiency, then management must conclude that the overall system of internal control is not effective.)

In other words, the final question is asking if all risks are controlled to acceptable levels and therefore objectives will be achieved.

2.2.2 The UK Corporate Governance Code 2018

Para 29. The board should monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness and report on that review in the annual report. The monitoring and review should cover all material controls, including financial, operational and compliance controls.

Paragraph 41 to the *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting* (2014) states, ' When reviewing reports during the year, the board should consider: how effectively the risks have been assessed and the principal risks determined; how they have been managed or mitigated; whether necessary actions are being taken promptly to remedy any significant failings or weaknesses; and whether the causes of the failing or weakness indicate poor decision-taking, a need for more extensive monitoring or a reassessment of the effectiveness of management's on-going processes.'

2.2.3 King IV (South Africa)

Principle 11 para 9 states disclosures that should be made in relation to risk.

2.3 The opinions

Considering the above, I've decided that the overall opinion to the Audit Committee (we'll assume one exists) will answer the question:

- Will the organization achieve its objectives?

(In practice: has the organization achieved its objectives; is the organization achieving its objectives; will the organization achieve its objectives?)

If the answer is 'YES', this implies the achievement of the organization's objectives is not being threatened by known risks (that is, the overall system of internal control is effective). If risks are found which may only hinder the achievement of the objectives (for example inefficiencies are found), a 'YES WITH EXCEPTIONS' opinion can be given.

Supposing risks are found which are not being managed to acceptable levels (that is, they are above the board's risk appetite)? In COSO's terminology, 'major deficiencies' exist. The audit committee is probably going to want to know more, and I suggest three further opinions are needed:

- Has management established a proper internal control framework? That is, has management: specified their objectives, identified the risks threatening these objectives and established controls which should reduce the risks to acceptable levels (risk appetite)?
- Is the internal control framework operating? Are these controls sufficient and operating to bring the risks to below the risk appetite and ensure the achievement of the related objective?
- If the internal control framework is not operating properly, is action being taken which will bring the risks to below the risk appetite and ensure the achievement of the objective?

The opinions to be given are defined by the assessments in the table below:

Opinion on	Assessment		
Has management established a proper control framework? That is, has management: specified their objectives, identified the risks threatening these objectives and established controls which should reduce the risks to acceptable levels?	Thorough processes have been used with the result that necessary controls to risks have been established. The objective will be achieved if the controls are operating.	Processes have been used, but there are some deficiencies which are not judged sufficient to prevent the achievement of the objective.	Inadequate, or no, processes have been used and, it is probable that the objective will not be, OR is not being achieved
Are these controls sufficient and operating to bring the risks to below the risk appetite and ensure the achievement of the related objective?	Controls are sufficient and are operating to bring risks to below the risk appetite. (although some action may be required – note in "Supplementary issues".) No more monitoring is necessary than is done at present The objective is being achieved.	Controls are sufficient and are operating to bring most risks to below the risk appetite. However, some risks are not below the risk appetite but are not judged sufficient to prevent the achievement of the objective. Some additional monitoring may be required (see the report for details)	Controls are not sufficient and/or are not operating to bring risks to below the risk appetite. It is probable that the objective will not be, OR is not being achieved. Major improvements are required to the monitoring of controls
Is action being taken which will bring the risks to below the risk appetite and ensure the achievement of the objective?	The action being taken will result in all risks being mitigated to below the risk appetite.	The action being taken will still leave some risks above the risk appetite but these are not judged sufficient to prevent the achievement of the objective.	No action is being taken, OR Insufficient action is being taken to mitigate risks to below the risk appetite.
Opinion:	**YES**	**YES WITH EXCEPTIONS**	**NO**
Report as:	**No deficiency**	**Deficiency**	**Major deficiency**

2.4 When is the opinion presented?

Looking at our definition of internal auditing we now know how the opinion is given.

When is the opinion presented to the audit committee? When it is required by them? This should be at least annually, so that they can make any declarations about the internal control framework but an opinion may be required at each audit committee meeting.

2.5 How is the opinion reached?

The audit opinion is 'rational' that is; based on verifiable facts, viewed without bias. Thus there are two stages to reaching an opinion:

- Examination of the internal control framework set up by management, to ensure it is complete.
- Testing of the controls within this framework, to ensure they are operating as intended.

In practice we will need to carry out these two stages in many parts of the organization and therefore divide the examination and testing into 'internal audits' each giving the opinions we have considered above on specific areas within the organization.

Before we can carry out audits, management need to establish the proper internal control framework and that's the next chapter...

3 Establishing the internal control framework

3.1 The stages

What should the Board and management do to set up the internal control framework?

The stages are as follows:

- The Board and management specify the objectives of the organization.
- A system for measuring the threat that a risk poses to the objectives has to be established.
- The board then defines a risk appetite in terms of this measuring system, which therefore provides a measure of an 'acceptable' risk.
- The Board and management identify all the risks which threaten these objectives, and score them.
- Management establishes internal controls to reduce, or remove, the risk threat.
- Management scores the residual risks (that is risk after controls are applied) to ensure they are below the risk appetite.
- The objectives, risks and controls are formally recorded in a *Register* with their scores.

The stages above primarily refer to process risks (and opportunities). Because decision risks are not easily predicted, they can only be generally managed by proper training and good information. Decision risks should be included under all objectives in the 'Objectives, risks and controls register' (details later).

I get the impression that risk managers don't like trying to measure risks and put them in a register. I can understand this if risks are just listed without any reference to the objective which is threatened or to the controls managing it. Scoring of risks is also imprecise and can't be taken as accurate.

However:

- Many organizations are required to report publicly their 'Principal Risks'. This implies some sort of scoring in order to sort risks and determine those which are principal.
- Since organizations have to report their principal risks, Audit Committees will want an opinion from internal audit that these are being managed to a level approved by them (They may have to report that they have done this).
- Internal Audit will therefore wish to direct their resources to check those internal controls which manage the principal and other high risks affecting the most important objectives. Thus there needs to be some sort of 'Audit Universe' driven out of the organization's objectives on which to base the audit plan.

So we need to measure risks.

3.2 Measuring risks

3.2.1 Scoring

We 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.

In order to decide the significance of each risk we need to 'score' them.

One common method of scoring risks, which is simple and effective, is to consider two characteristics:

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

There are several methods for measuring consequence or likelihood. One of the most common is to apply one of five levels to each characteristic, defined as below:

If the consequence when the risk occurs is:		The likelihood of the risk occurring is:		Score
To close down the organization, or a significant part, for a very long period	OR	Almost certain	Then the measure is defined to be	Very high (5)
To prevent the organization achieving a major part of its objectives for a long time		Probable		High (4)
To stop the organization 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 organization. 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 one of our lorries used to deliver famine relief 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.

3.2.2 Measuring the effect of controls

Risks are scored before and after taking account of the internal control 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.

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 may be residual risks, 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 objectives will be achieved because these controls are properly managing risks, the internal audit plan should be chosen on the basis of *inherent* risk, not *residual* risk. However the residual risk is useful because:

- It is the only measure we may have from risk workshops.
- It checks our scoring of the inherent risks. For example, a residual risk with a 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.
- In a numerical scoring system the difference between the inherent and residual risk scores is known as the *control score*, the assessment of control effectiveness, or the control co-efficient. The higher the control score, the more important the control. Since risks now have a numerical value, they can be sorted to show the greatest inherent risks, greatest residual risks, or those with the greatest control scores.

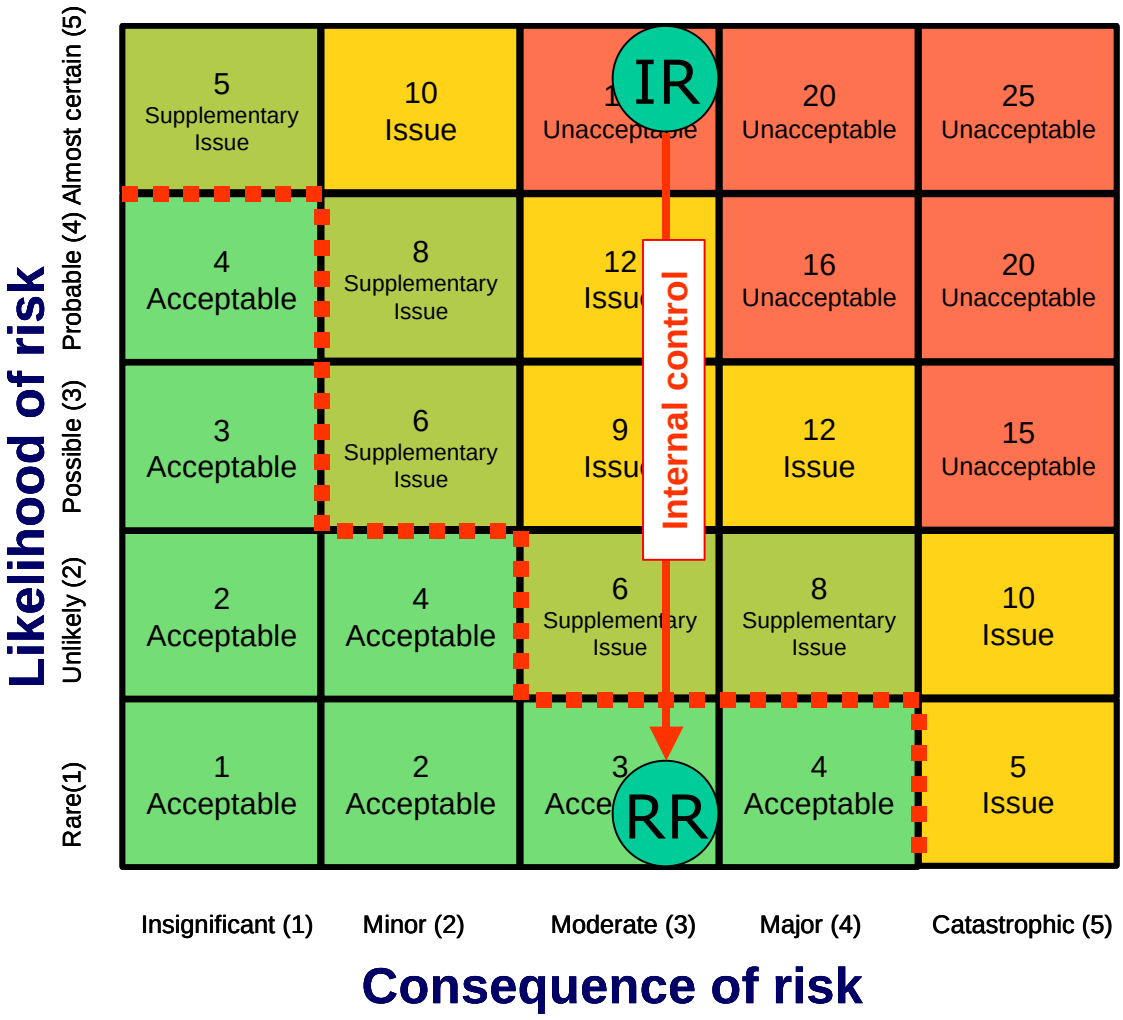
In organizations with several operating units, such as overseas subsidiaries, risk consequence may be scored in relation to that unit's value as well as in relation to the organization as a whole. Thus a risk causing catastrophic failure of a small subsidiary may score a consequence of 5 in the subsidiary's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

3.3 What risks is the board prepared to accept?

We have talked about managing all risks to acceptable levels, sometimes called the 'target' level. Now we have scored risks before and after internal controls we can begin to define the organization's 'risk appetite'.

One method of deciding which risks to accept is to place them on a grid of likelihood and consequence (see Fig. 2 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.

This is a rather mechanistic approach, not liked by many in the risk management community. However, it is a 'coarse' filter to detect the most significant risks which require a check to ensure the internal controls managing them are effective.



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 has 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.

If we have a *residual* risk in an 'unacceptable' or 'issue' combination then this:

- Gives a 'NO' opinion against our control question.
- Is a 'major deficiency' in COSO terminology

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

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 objectives will be met by the action of the controls in operation.**

3.4 Specifying objectives

We established in chapter 1 that we couldn't identify risks without specifying the objectives which they threatened. The top-level objectives will be specified by the Board of Directors (or equivalent). Some may be specified by any charters which established the organization, for example charities will have charters which set out its objective(s), for example, ' Relieve famine in central Africa'.

For a commercial company, the top-level objectives may be similar to:

1. Set up a strategy to deliver the objectives of the organization
2. Maintain profit of existing business
3. Develop the business
4. Operate within laws and regulations
5. Trade responsibly
6. State how responsibilities are met
7. Maintain support functions to deliver the objectives

While these objectives are applicable to the board, managers and staff will have objectives which are sub-objectives of the above. We would expect all these objectives are included in targets for the appropriate staff, in order to ensure they are achieved.

It is possible that your organization will not have defined any objectives although there will probably be the unwritten objective, 'To survive'. So your first task is to persuade the board to specify its objectives before identifying the risks threatening the achievement of those objectives.

We consider in a later section how these objectives and sub-objectives fit together with the risks which threaten them and the controls which manage them.

3.5 Identifying risks

3.5.1 The role of management

We have seen that the role of management includes:

- Identifying what risks exist.
- Scoring these risks (inherent risk score).

In some organizations management will set up a framework to identify and score risks, possibly appointing 'risk managers' to help. In other organizations, the internal audit activity will be asked to help, and in the remainder not much will happen at all.

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 organization.

Management may consider the identification of risks as an unnecessary bureaucratic exercise and it is therefore very important to drive the risks out of their objectives. They will hopefully understand that identifying risks and controlling them is an essential part in achieving their objectives.

3.5.2 The role of internal audit

We've learnt that:

> **Internal auditing provides an independent and rational opinion to an organization as to whether it is likely to achieve its objectives, based on the management of opportunities and risks.**

Which I consider to be 'Objective focused internal auditing'.

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

However, internal audit may assist in the identification of risks and advise on controls, provided this does not affect their objectivity and they take no role in managing the risks.

3.6 Finding the significant risks

3.6.1 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.

There are three basic methods of determining risks:

- Interviewing
- Risk workshops
- The accounts

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

3.6.2 Interviewing

The output from an interview is an individual's view of the risks hindering their objectives within the organization. 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 categorize.
- 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 B.

3.6.3 Risk workshops

The output from a risk workshop is a list of risks, which could threaten the objectives being considered, with a measure of their consequence and likelihood.

Risk workshops can be used:

- To persuade participants that an understanding of risks is not a bureaucratic exercise but necessary to achieve their objectives.

- With the most senior people in an organization, 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 concerns they may have about risks and controls.

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

Details of how a risk workshop can be run are included in appendix C.

3.6.4 The accounts

We should examine the accounts of the organization, 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 past failures show this trust might be misplaced.

3.7 Identifying controls

When management has defined the risks to their objectives, with or without internal audit's help, they will have to determine the responses to these risks.

As we noted in chapter 1, there are four possible types of response:

1. Terminate: stop the activity giving rise to the risk
2. Transfer: insure against the consequences when the risk occurs. (IA will need to check the terms of the insurance).
3. Tolerate: accept the risk. (IA will need to check if any contingency plans are required).
4. Treat: introduce processes (controls) to reduce the risk. (IA will need to check that these controls are sufficient and operating).

In practice, many of the required controls will be operating - especially if internal audits have been carried out! Some new controls may be required, especially to ensure the proper communication of the organization's culture and strategy.

3.8 Organizing objectives, risks and controls

3.8.1 What we have

At this stage we should have:

- A method for scoring the risks.
- A risk appetite set by the board.
- Objectives, risks threatening these objectives and controls which should reduce the risks to acceptable levels.

We can now go ahead and consider how the organization is to record its objectives, risks and controls, so we don't have a long unstructured list which cannot easily be used as the basis of an audit program.

We have seen that we will probably need to break down the objectives into a hierarchy (levels) until we come to a level where there are only a few risks threatening each objective. We can then audit the controls managing these risks.

3.8.2 Level 1 objectives and risks

Let's take an example – a charity with the top level (level 1) **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 organization. I should state that I have no experience of this type of charity!).

The significant 'top level' (level 1) **risks** might include:

- No clear strategy as to how to achieve our objective.
- Unable to predict where and when famines will occur.
- Unable to obtain food.
- Unable to deliver the food to the starving.
- Do not have the staff and systems to support the operation

These risks can be arranged in a hierarchy (appendix D).

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 the routes for the lorries were safe from bandits.

3.8.3 Level 2 objectives and risks

So we need to break down the objectives further until we get to a level where we can identify risks and controls which can be audited. How? We've seen that risks hinder objectives, so the next level of objectives is to overcome the risks identified.

Taking our example:

Risks to level 1 objective	Related objectives (level 2)
1. No clear strategy as to how to achieve our objective.	Devise a strategy for the next five years to deliver our objectives
2. Unable to predict where and when famines will occur.	Set up a system which enables us to predict famine areas
3. Unable to obtain food.	Set up agreements with donors to obtain food
4. Unable to deliver the food to the starving.	Establish a supply chain to ensure prompt delivery of food to the highest priority areas
5. Inadequate resources to deliver the objectives	Employ sufficient, suitably qualified staff using sufficient resources

Let's carry on to the next hierarchy (level 2) for risk/objective 4:

'Establish a supply chain to ensure prompt delivery of food to the highest priority areas'.

One *level 2 risk* to this objective is:

'Don't distribute food efficiently and effectively'.

One *level3 objective* arising from this risk is:

'Arrange land transport'. (There are other objectives).

Appendix D shows the hierarchy (omitting some risks due to lack of space).

The mind map in the accompanying spreadsheet (http://www.internalaudit.biz/files/introduction/rbiaintroduction.xlsx) shows the objectives, risks and controls - see the branch ' Unable to deliver the food to the starving'.

3.8.4 Level 3 objectives and risks

We have now reached a level where there are only a few risks threatening each objective and the internal control required is nearly identical to the objective. So, we can identify the internal controls we can test in an audit.

Risks to level 3 objective 'Arrange land transport'	**Internal controls managing risks**
1. Insufficient drivers	List of drivers available for hire is kept by the compound office
2. Routes become impassable due to the weather (*decision risk*)	Work with other agencies and the military to plan routes
3. Routes become impassable due to bandits	The army escorts convoys
4. Bandits attack lorries (*decision risk*)	All convoy workers to undergo training on making decisions about how to react in the event of an attack
5. Fuel not available for lorries	Fuel is stored in the compound
6. Labor to load lorries not available	The warehouse provides loaders
7. Insufficient lorries to move food inland	Eight lorries are available for transport
8. Lorries break down	Two mechanics are on the permanent staff
9. Do not know where camps are	Charity has established a network of reliable local people with access to mobile phones
10. Do not know where food is required most urgently	Charity has established a network of reliable local people with access to mobile phones

3.8.5 A hierarchy of objectives, risks and internal controls

So we have now built up three levels of objectives and risks by

- Looking at the risks to the top objective.
- Identifying the responses required to these risks, which we have taken as *level 2 objectives*.
- Determining the risks to these *level 2 objectives*.
- Identifying the responses required to these level 2 risks, which we have taken as *level 3 objectives*.
- Determining the risks to these *level 3 objectives*.
- Identifying the responses required to these level 3 risks, which we have taken as *internal controls*.

This seems a complicated method for getting to the internal controls which we need to test. However:

- By starting at the top and working down we are unlikely to miss major objectives and risk areas.
- We have a framework in which we can link any internal control we test back to the main objective, thus we can show management how internal audit can give them confidence about the control over the risks threatening their objectives.
- This framework also enables us to count the risks at each level after we have scored them. Thus we can report to the Audit Committee what percentage of risks at each level we have checked, thus giving an objective measure of the Internal Audit Department's work.
- The framework can be shown as a 'mind map' (see book 2 and the ORCR spreadsheet for this book) which gives an overall view of the objectives and risks.
- Once set up, the framework only needs to be modified as the objectives of the business change. It is independent of the departments and people in the organization, and so, when they change, we don't have to change the map, only the owners of the objectives.
- By scoring the risks relating to each objective, we can identify the objectives threatened by the most significant risks and audit these first.
- We can define audits in terms of the objectives included in that audit. Thus enabling us to easily identify our audit coverage.

3.8.6 An alternative method

When I was a trustee for a small charity providing 60 houses for the elderly, I had to compile a risk register. The charity is an almshouse charity, with standards available from the Almshouse Association. I used these standards to create a three level hierarchy of processes and generated risks from the standards. These were then combined with risks compiled by the Board of Trustees. Details are available on www.internalaudit.biz site.

Standards may be applicable to parts of an organization, such as IT, where the Control Objectives for Information and related Technology (COBIT®) standards can be applied.

3.9 Recording the risks

3.9.1 What we've got so far.

Management will now have a list of objectives, risks threatening them and controls managing the risks. Each risk will have inherent and residual risk scores

It will have taken some time, and considerable effort to reach this stage. Depending on how well management has built up the internal control framework, we may have some problems:

- 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. Try linking the work to the achievement of their objectives (and possible bonus!).
- We don't know if the organization has captured all its risks, and has a record of them.
- Risks may not have been identified with the objectives they threaten.

- Many risks will focus on new projects which may not have clear objectives. When it comes to audit planning each project will have to be evaluated to determine its objectives and assess its risks.
- Some risks will be very broad covering most, if not all the organization. Such risks include:
  - Poor decision making.
  - The inability to recruit good staff.
  - The lack of contingency plans.
  - Fraud.

In practice these are included as additional processes under the level 2 objective, 'Employ sufficient, suitably qualified staff using sufficient resources' but considered for inclusion in all audits. Appendix K gives some ideas, including both process and decision risks..

- One risk that will be highlighted is 'the loss of the organization's reputation'. However, an organization doesn't lose its reputation for no reason but from other risks, such as poor quality products, bad advice, and expensive products. So when this is mentioned as a risk, determine the underlying risks.
- Any 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.

3.9.2 The Objectives, Risks and Controls Register

Since risks will have to be scored and sorted, they are best input into a ‘database’ which we have referred to as the *Objectives*, *Risks and Controls Register (ORCR)*. This can be held in a spreadsheet (for example ‘Excel’), or database program (for example ‘Access’). Appendix E shows part of this database, held on a spreadsheet. (Those appendices which show the risk register can only show part, with some columns and rows omitted.) You need to download the spreadsheet from Book 1 at https://www.internalaudit.biz/files/introduction/rbiaintroduction.xlsx in order to view the ORCR and associated worksheets and fully understand this book.

The features of the ORCR spreadsheet are:

- Columns for all levels of objectives, risks and controls. Since each risk is to be scored and sorted, each row has to be complete so the objectives to which it is attached are repeated in the appropriate columns. If an objective is threatened by several risks it is repeated. If a risk affects more than one objective, it is repeated.
- Inherent and residual risk scores. The risk is given scores for consequence (Cons) and likelihood (Like), before and after controls. These two scores are multiplied together to give the significance score (Sig). We can calculate the control score as the inherent risk score minus the residual risk score. This gives a measure of the importance of the control, and therefore the priority we should give it when decided when to audit it.
- The source of the risk. This is important to demonstrate its authority.
- The function with overall responsibility for achieving the objective. The spreadsheet has an example hierarchy of functions within the charity.
- The control owner who has responsibility for ensuring the control is operating.
- A column for 'Process', which is included to link the objective/risk/control with the tasks which deliver the control, such as sales cycle, purchases cycle and payroll. The spreadsheet has an example hierarchy for processes. Grouping risks by process can help allocate objectives, risks and controls to the audits which will examine them.

3.9.3 Updating the register

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

The ORCR needs to be held independently, to ensure changes are correct. This might be risk management in a large organization, or could be internal audit.

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

3.9.4 The next steps

The Objectives, Risks and Controls Register forms the foundation of the internal control framework and provides the basis for internal audit work.

So we are now able to consider what internal audit work needs to be done and how to do it.

4 The Risk Based Internal Audit

4.1 What is risk based internal auditing?

My definitions were summarized in chapter 1 as

- Opportunities benefit and risks threaten the achievement of objectives.
- Internal controls manage opportunities and risks in order to maximize the likelihood and impact from achieving objectives
- Internal auditing provides opinions about whether objectives are being or are likely to be achieved based on the effectiveness of internal controls.

So if you want your organization to achieve its objectives, you have to check all the controls aiming to reduce all the risks which threaten the achievement of those objectives. Internal auditing aims to do this. The term *Risk based internal auditing* arose from the need to distinguish internal auditing in this widest sense from 'traditional' internal auditing:

- Risk based internal auditing starts with ***all*** the objectives of the organization and provides an opinion as to whether these objectives will be achieved by the risks threatening these objectives being reduced to an acceptable level by internal controls.
- 'Traditional' internal auditing is considered as being limited to considering controls over financial and fraud risks and, possibly, IT risks.

So risk based internal auditing is identical to the internal auditing expected by modern standards, that is involving *all* the risks threatening all the organization's objectives. I believe therefore that we should not concentrate on implementing *risked based* internal auditing but on expanding the narrow interpretation of *internal auditing*. Ideally we should forget the term *risk based internal auditing* and make *internal auditing* what it should be. However, to avoid confusion, I will continue using *risk based internal auditing* on the website and books but think of it as internal auditing with the boundaries pushed out.

So what are the boundaries?

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

So what are the boundaries ***from*** which we expanding internal audit?

- That depends entirely on our existing internal audit function!

The changes which might result from pushing out the boundaries are detailed in chapter 9. The main difference is that risk based internal auditing (RBIA) is driven by the organization's list of objectives and risks, not internal audit's. I prefer the term 'Objective focused internal auditing' as I believe this describes the foundation on which internal auditing should be concentrating.

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

This means that the organization's risks determine where and when internal audits take place. There is no separate list of internal audit's risks, no separate schedule of internal audits to be carried out on a cyclical basis and no list of systems to be audited.

Since we are dependent on management's list of objectives and risks (the ORCR) doesn't this affect internal audit's independence? No, because our first task is to make sure the ORCR is accurate and complete!

Chapter 5 covers the checking of the ORCR. Chapter 9 looks at the impact of introducing RBIA in greater detail.

4.2 The RBIA stages

In chapter 2 we decided that four opinions were required to report to the board:

- Will the organization achieve its objectives?
- Has management established a proper internal control framework? That is, has management: specified their objectives, identified the risks threatening these objectives and established controls which should reduce the risks to acceptable levels?
- Are these controls sufficient and operating to bring the risks to below the risk appetite and ensure the achievement of the related objective?
- Is action being taken which will bring the risks to below the risk appetite and ensure the achievement of the objective? (Optional, depending on the previous opinion).

Two audit stages are therefore required to give these opinions:

- Examination of the internal control framework set up by management.
- Testing of the controls within this framework.

In practice we need to split the examination and testing stages into individual audits, targeted at the risks with the highest inherent scores. So we need to plan these audits. The flowchart on the next page shows the main activities in the planning process carried out by internal audit management. It also shows the main activities involved in an individual audit.

The first step in RBIA is to establish that an Objectives, Risks and Controls Register exists!

The second step is to check that it is suitable as the basis for audit planning. This involves establishing the organization's 'Risk Maturity'.

A diagram of the processes is below. Note that:

- The ORCR should be regularly updated (that is, at least monthly) to take account of new objectives, opportunities and risks.
- The annual and 3m internal audit plans should change if new objectives and risks require immediate attention.
- The report to the board or Audit Committee may be more frequent than one year.

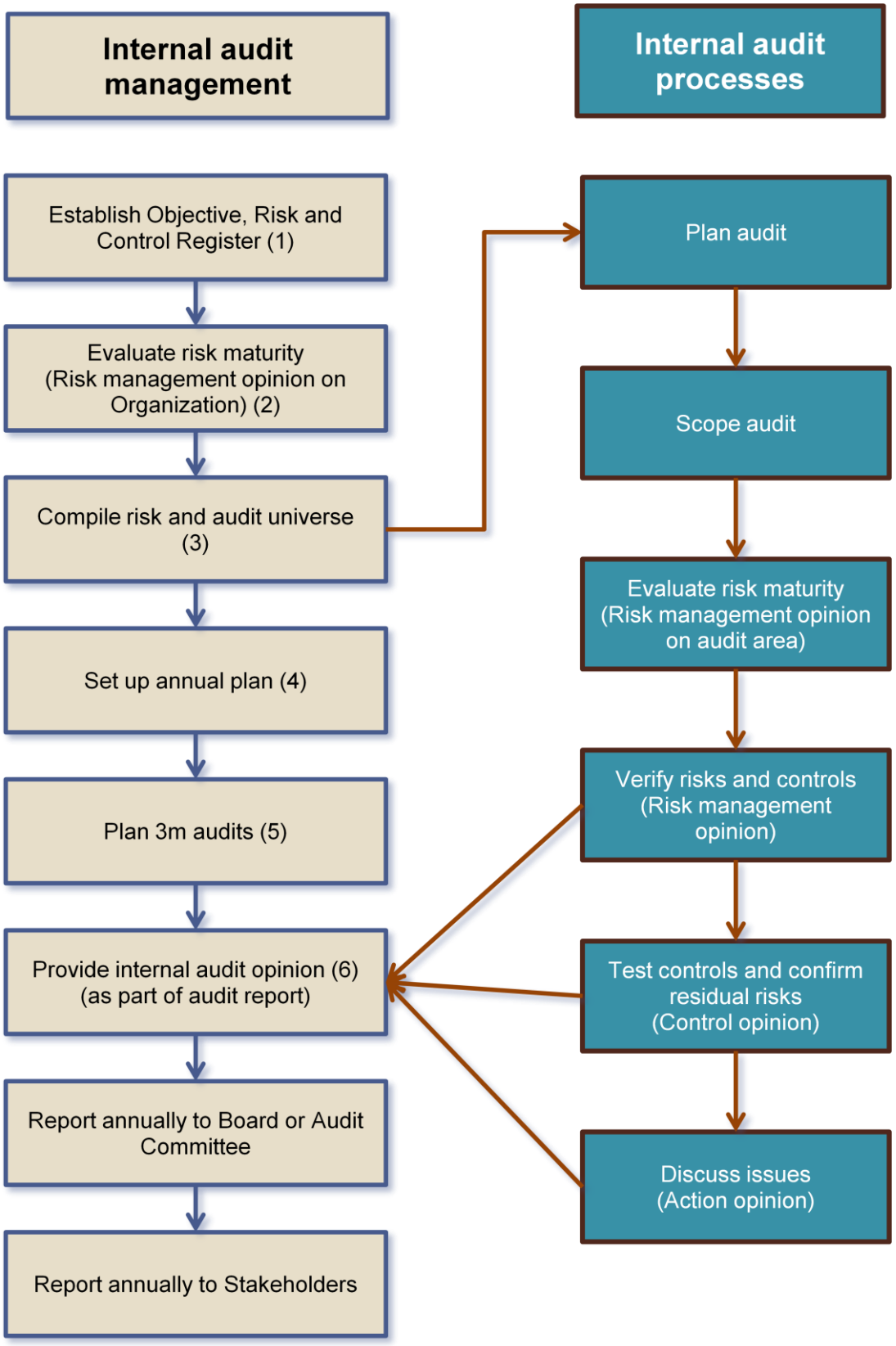


Fig. 3 The risk based audit processes

5 Risk maturity

5.1 Assessing the organization's risk maturity

We've seen

- How risks can be measured
- How this measure can be used to decide whether risks are acceptable
- That managers own risks and it is their responsibility to control them.
- That internal auditing provides an opinion, to management, as to whether these risks are properly controlled to within the board's risk appetite and that objectives will therefore be achieved.

So internal audit can only provide an opinion where managers have determined their objectives and the opportunities benefiting them and risks threatening them.

In an ideal world, internal audit will have assisted managers to build a risk register (ORCR) which can be the basis of a risk and audit universe (RAU).

In the real world we may not get the opportunity to influence the compilation of the ORCR. 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 organization understands risks and has implemented risk management is known as its *risk maturity*.

5.2 Levels of risk maturity

The Chartered Institute of Internal Auditors (IIA – UK and Ireland) publication on 'Risk Based Internal Auditing' defined five levels of risk maturity: risk enabled, risk managed, risk defined, risk aware and risk naïve. In March 2019 this document was replaced by a Practice Guide, 'Assessing the Risk Management Process', which uses different terminology. I'm not updating this book as the basic principles have not changed but you may wish to obtain the book for further information. 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 organization fits!

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 organization. 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 deficiencies 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 deficiencies 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 ORCR. The internal audit activity will act as a consultant to facilitate the compilation of a complete ORCR from lists risks already compiled by managers.
>
> The quality of risk management may vary across this type of organization. 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 deficiencies are found.

Risk aware: (Scattered silo approach to risk management)

> No ORCR 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 organization, it will be necessary to promote, or provide consultation on, the establishment of a risk management framework

5.3 The impact of risk maturity

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

1. For organizations that are subject to regulations concerning the adequacy of risk management, the level of risk maturity in risk aware and risk naïve organizations is not acceptable, and we should report this to the audit committee.
2. If our organization has this level of risk maturity, we don't have a reliable ORCR 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 ORCR necessary but it only encourages management to continue believing that internal auditors own the risks!
3. Risk driven individual audits are possible, without reference to an ORCR. 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.

The impact of the risk maturity of an organization on the internal audit activity 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 and its impact on the achievement of objectives.

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

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

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

5.4 Reliability of the risk register

5.4.1 Objective of this step

To provide the opinion, for the whole organization: Has management established a proper internal control framework? That is, has management: specified their objectives, identified the risks threatening these objectives and established controls which should reduce the risks to acceptable levels (risk appetite)?

5.4.2 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 organization such as training, risk workshops, questionnaires about risks and interviews with risk managers.
- Ask for documents which detail:
  - The objectives of the organization.
  - Responses to the COSO (US) or FRC (UK) requirements or any national legislation.
  - 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.
  - The organization's risks, preferably structured in some way which enables an opinion to be made as to the completeness of the risk register.
- Examine the documents, check that procedures are adequate and have been followed, throughout the organization.
- Complete the checklist (spreadsheet appendix F).

5.4.3 The risk maturity checklist

Appendix F provides details of the questions to ask, which are taken from,' IIA Guidance Note – An Approach to Implementing Risk Based Internal Auditing' (Now replaced by a Practice Guidance). I have taken this appendix and modified it using COSO and ISO 31000:2009 (updated in 2018). This modified checklist is in the spreadsheet.

- The first three columns relate to questions derived from ISO 31000, COSO and the IIA. These are the controls required to ensure a proper risk and controls framework. (You should obtain the IIA Practice Guidance and updated ISO 31000 if you want to be certain of following current guidance, but the principles in Appendix F still apply).
- The next column contains the charity's controls to achieve the framework.
- The next four columns show the tests and results designed to check whether the controls are sufficient.
- The last columns contain the conclusions from the tests.
- Since the charity is small, the risk management function is carried out by Internal Audit.

5.4.4 Opinion

Using the checklist in appendix F (spreadsheet) we can then reach a conclusion as to the suitability of the ORCR 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 organization, 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.
- Note that the opinion will only apply to the parts of the organization we can test. It is possible that subsidiaries, divisions, or business units that we have not been able to visit are not at the same level of risk maturity as 'Head Office'. For this reason, appendix F will be used in individual audits to assess risk maturity.

For the purposes of this book we will assume that the ORCR can be used as the basis of the risk and audit universe. Book 2 provides details of how to compile a risk and audit universe where the risk register cannot be used.

6 Compiling the risk and audit universe

6.1 Objective of this step

To produce a Risk and Audit Universe (RAU), which is based on the ORCR, and allocates the risks to audits which will provide the opinions specified in chapter 2. (An example format for the risk and audit universe is shown in appendix G.)

The tasks involved in using the ORCR to derive the Risk and Audit Universe (RAU) are shown below.

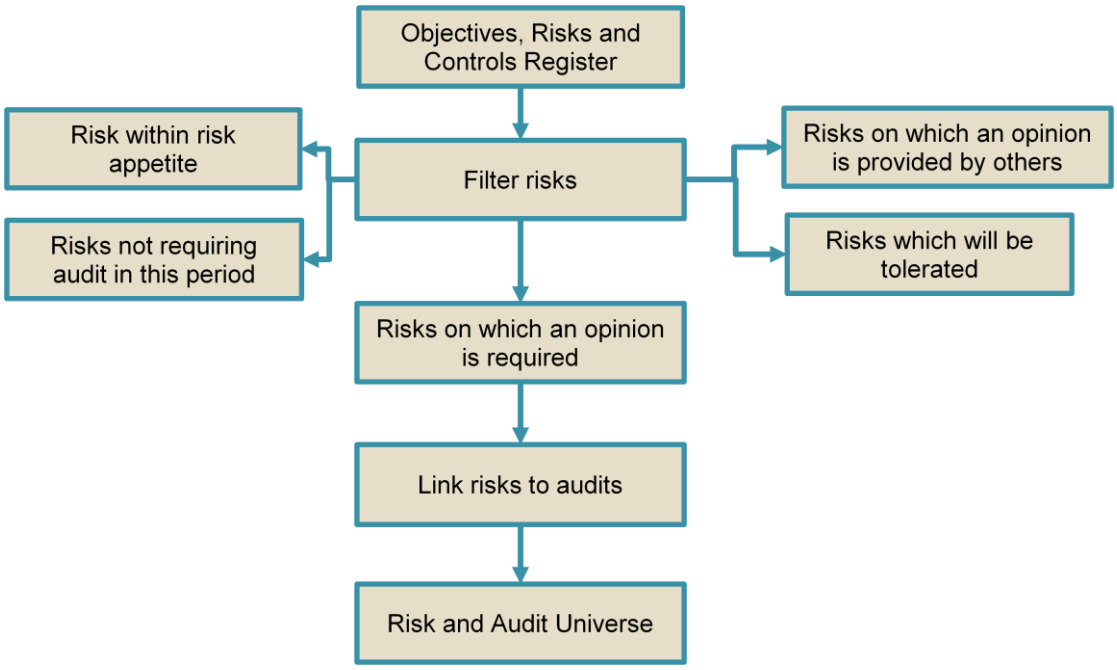


Fig 4 Compilation of the RAU

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:

- The inherent risk is within the risk appetite of the organization and requires no further work.
- Management considers 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 has *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 (Chief Compliance Officer, for example). The organization'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. 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.

6.3 Allocate risks to audits

6.3.1 Categorize the risks

At this stage we have a list of risks, grouped by the objectives which they threaten (see spreadsheets linked to this book and Book 2). These spreadsheets (including E ORCR) have columns for several categories including:

- **Function** The function affected by the risk (may be the division/operating unit/function) because it has the responsibility of delivering the related objective.
- **Internal control owner:** The job title of the person responsible for operating the control, who will normally be in the function affected.
- **Process**: The process in which the internal control operates (such as marketing, research, supply chain, accounts payable). The function concerned will normally be responsible for operating some of the process.

6.3.2 Group the risks

Theoretically we could start with the highest scored inherent risk, check that the control(s) mitigating them are working, report our opinion and move onto the next highest scored risk. This would be very inefficient, so we need to group risks and check these in one audit.

Risks may be grouped into audits by:

- **Function**; useful for 'off-site' audits such as overseas subsidiaries, stores or branch offices.
- **Internal control owner:** Useful for risks which are the responsibility of senior managers, such as the Managing Director.
- **Process**: useful for most audits, since this is probably the most efficient way of auditing and corresponds to the familiar 'systems based' audits.

The linking of risks to the audits which will provide an opinion is a crucial stage, as it will determine the scope of the individual audits. Examples are shown in the spreadsheet G (RAU), such as linking all the risks associated with the 'Distribute food' process to form a 'Transport of food to camps' audit.

Ensure that the management of those risks which may not be linked to processes or business units, such as external risks, is included in the audit plan.

Where the response to risks is not treatment (controls), other action might be required. This is noted in the *Control* column:

- Risks are tolerated: the audit committee should be aware of this and the possibility of providing an opinion on contingency plans considered.
- Risks are transferred (for example by insurance): an opinion should be provided as whether all risks have been transferred and robust processes exist to ensure any appropriate new risks are captured. Where it is considered that risks have been outsourced, for example information system risks to a third party supplier, it will be necessary to identify the new manager of the risk and that any compensation for their failure to manage risks is adequate and set out in the contract.
- Risks are terminated: an opinion might be necessary as to whether the risk has disappeared.

Providing an opinion on the management of some risks, such as 'a major disagreement among directors', may be considered impossible. However, this may mask a reluctance to address the risk, or put in place contingency plans. Every risk should have a response; every response can be audited.

Consider the list of audits identified. Are any missing that the internal auditor would consider essential to check the management of significant risks? Their absence may indicate that some risks are missing from the ORCR.

Each audit group (that is risks to be covered by the same audit) is given a unique identifier. This may be a letter, or the function/owner/process linking the risks. This enables the spreadsheet to be sorted on this column in order for risks to be grouped by audit.

Objectives, risks and controls and audits are now linked and the resultant list is known as the *Risk and Audit Universe (RAU).* (It should really be called the Objectives, Risks, Controls and Audit Universe - ORCAU - but this is too much of a mouthful!) Examples are given in the spreadsheets accompanying this book (appendix G) and Book 2.

6.3.3 Small organizations

In a small organization, for example a small charity which has to produce a risk assessment by law, 'internal audits' will not be a realistic way to confirm risks are being managed.

In these organizations the response to each risk can be checked individually, and the result noted against the risk in the *ORCR*.

6.3.4 Systems audits?

So haven't we spent all this time and effort just to come up with 'systems audits'? The short answer is yes BUT:

- We will be auditing in areas outside the traditional financial systems audits, such as corporate social responsibility, research and major project approval, since the audits are based on examining internal controls in all the high risk areas of the organization.
- We will include opportunities as well as risks plus decision risks as well as process risks.
- We can see the relevance of every internal audit test, since it can be linked to the organization's overall objectives.
- We can form an opinion on the adequacy of the organization's response to all its risks.
- We can present an opinion to our stakeholders which states what proportion of risks we have examined.

6.4 The RBIA Documentation

6.4.1 The risk and audit universe (RAU)

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

- Audits in the current audit plan
- Risks, in order of the objectives they threaten.
- Risks, in order of their significance, using the inherent risk score.
- Risks associated with a particular process or function.
- Many other reports, including those showing resources, depending on the data held.

Having linked risks and audits, we can now begin to generate the audit plan, which is the subject of the next chapter.

We have now set up one of the two databases (G - RAU) which drive the methodology detailed in this book. The other database applies to individual audits.

6.4.2 The audit database

It would be theoretically possible to include all the organization's risks in the RAU but this may 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.

A 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 J (Audit Database) and the full version in the spreadsheet working papers (146workingpapers) 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.

6.4.3 Summary

The diagram below summarizes the important data 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.

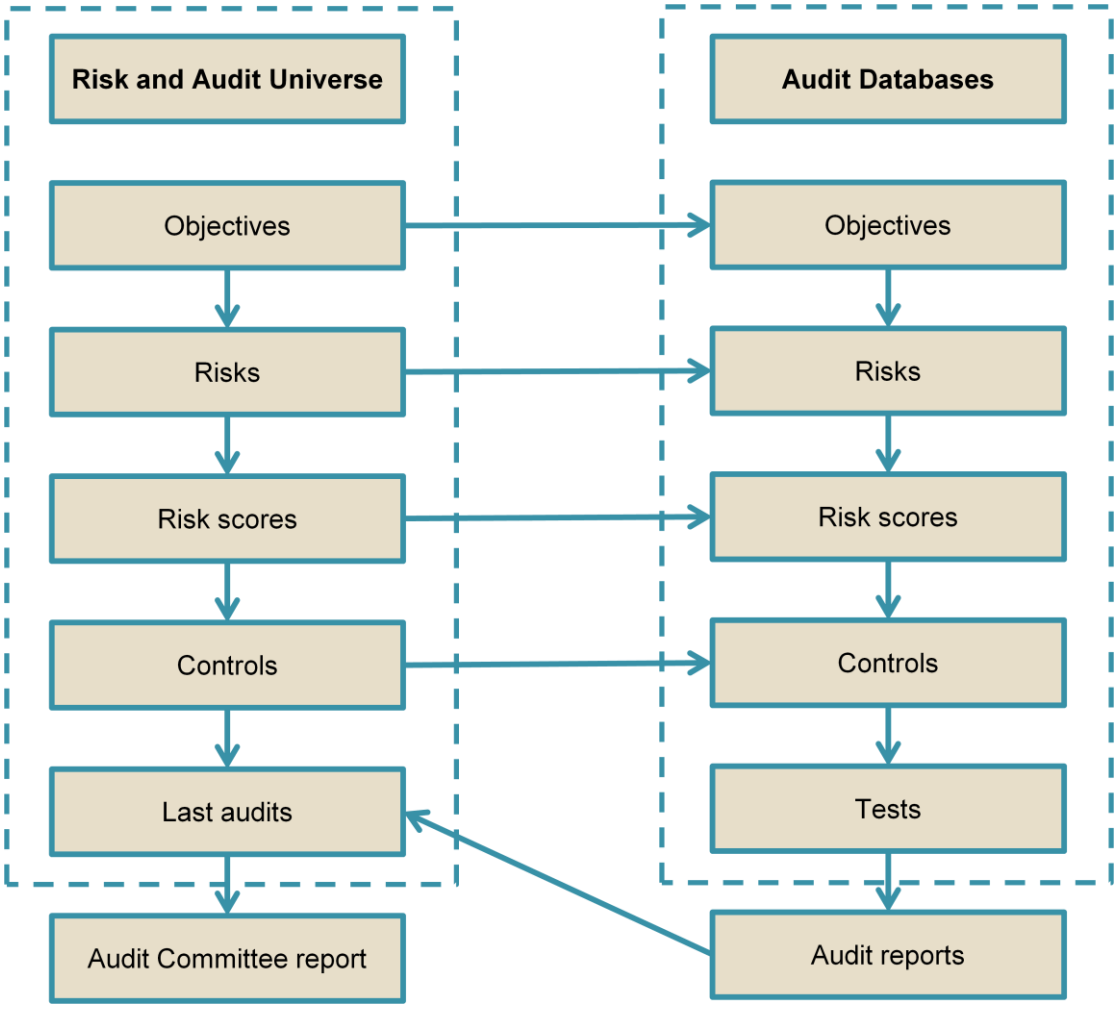


Fig 5 Audit documentation

7 The annual audit plan

7.1 Objective of this step

To produce a plan showing:

- Those audits required in the year.
- When they might be carried out.
- How long they are expected to take (days).
- The staff provisionally assigned to the audits.

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

7.2 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 organization's senior management (board, trustees) may require a plan to use as a target for the internal audit activity.
- Some regulations require an annual assessment 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. For example, in the US, we will need to ensure sufficient audit work has been done to complete the COSO 'Overall assessment of internal control template'. (See book 2 for more details).

7.3 Which audits to select?

We now have a Risk and Audit Universe (spreadsheet G) with each risk linked to an audit group. We also have the opinions from audits carried out last year. So what audits do we want to perform this year?

The basic principle will be to select those risks with the high inherent scores. One possible way of selecting audits would be to add up the scores of the risks and choose the audits with the highest total score.

There will be a range of risk scores and, in drawing up the audit plan, a policy will have to be established about which risks to cover and how often. It is unlikely that the board, or audit committee, will require assurance on the management of every inherent risk above the risk appetite, every year. They may require an opinion on the risks with a high likelihood of significant/catastrophic losses every year but other risks above the risk appetite every two or three years. .

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

The residual risk score is not used as a basis for the audit plan, as it is determined using the assumption that the internal control is operating, and it is this that we wish to audit.

In practice, a provisional list of audits will be discussed with senior management and the audit committee, as appropriate. The agreed audits will be input into the RAU, which is updated during the year (Appendix H worksheet)

7.4 How often 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 organizations this would require a large number of auditors, so a compromise has to be found.

7.4.1 Use a 'Heat map'

One possibility is to use our matrix (below). At the start of RBIA we would aim to audit the management of 'red' inherent risks is 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.

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

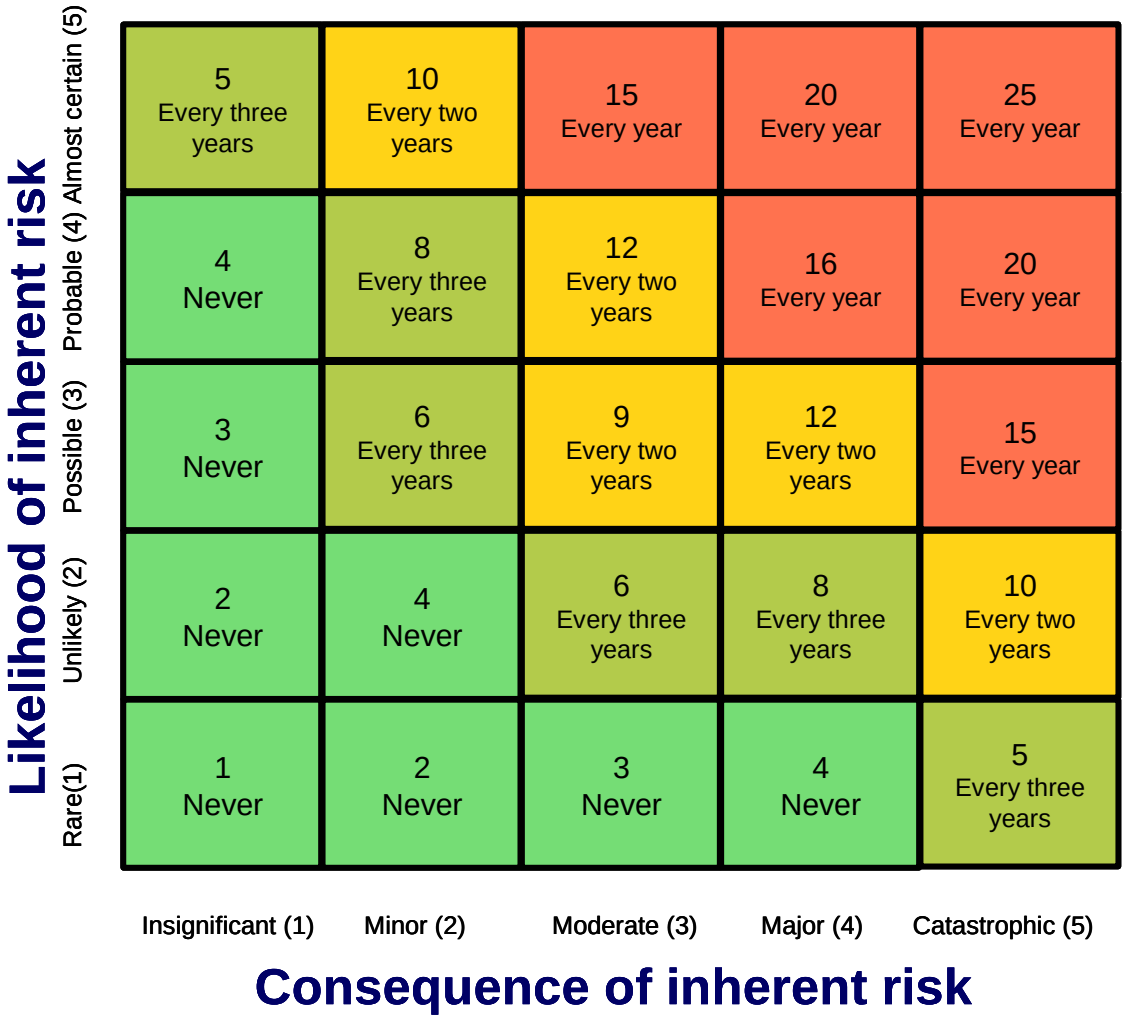


Fig. 6 Grid for the frequency of audits

7.4.2 Reduce the inherent risk score

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 inherent risk score, based on the time since the last audit, and the opinion, though this approach assumes no major changes in the areas concerned. For example:

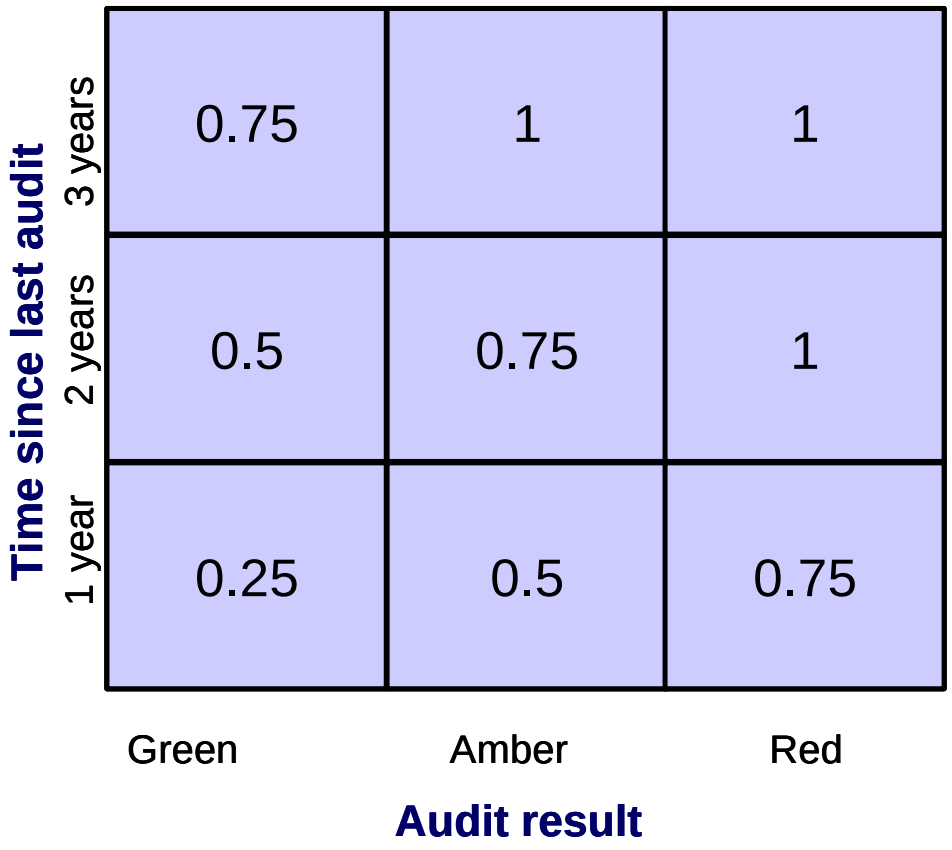


Fig. 7 Factors to reduce inherent risk scores

Audit result opinion: 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 one year ago and found not to be controlled (red), it would be scored with a significance of 12*0.75 = 8 when drawing up the audit plan.

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 (appendix H - full version in spreadsheet). 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.

7.5 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 organization's risks).

If resources are insufficient to complete the plan, prepared on the basis of internal audit's terms of reference, an increase in staff should be considered, alongside other options, such as reducing the number of audits.

If sufficient staff are not available, the audit committee should be informed of those risks not audited due to resource constraints and given the opportunity to decide on their preferred option.

When resources have been allocated, approximate timings and other details of the audit can be input to the RAU under the 'Next Audit' columns.

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 organization'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 or staff leave the department.

7.6 The ongoing risk and audit universe

We now have the **definitive** *risk and audit universe* of objectives, risks, controls and audits for 20X1 (appendix H). This database:

- Records the objectives and their related risks. It is updated at least quarterly by those managers who own the objectives. The impact on the audit plan should then be considered. It may be necessary to add audits where new, significant risks have been identified and remove those where risks are considered to have diminished. In particular, it will be necessary to add new major projects to this list.
- Shows the 'owner' of the risks, that is, the person directly responsible for ensuring the risk is being properly managed
- Is used to decide on those risks, with management, where it requires audits to give an opinion whether the objectives are likely to be achieved based on risks being managed to acceptable levels. This includes the addition and removal of audits resulting from the periodic updates of risks and their scores.
- Shows the risks whose management will be checked by each audit.
- Indicates the agreed timing (month or quarter) of planned audits.
- Shows the status of the audits for the current year (unplanned, planned, fieldwork, reporting, complete).
- Indicates the achievement of milestones (issuing the final audit report).
- Shows the results of previous audits.
- Forms the basis of next year's plan, after updating with the results of audits from this year.
- If required, shows the controls and monitoring controls which manage the significant risks in the RAU. These will otherwise be shown in the individual audit databases.

- Generates Internal Control Questionnaires for managers to confirm the proper operation of controls for which they are responsible.

7.7 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:

- Objectives, where an opinion will be provided about the likelihood of achieving them, based on the effectiveness of the risk management processes controlling the threats to the achievement of those objectives. Audits in the plan will confirm the proper operation of these risk management processes
- Objectives where an opinion will be provided but based on audit work from previous years, plus limited follow-up work where desirable.
- Objectives where consultancy work will be carried out to assist management in reducing the residual risks to below the risk appetite.
- Any objectives not covered, due to policy or resource constraints.
- Confirmation that the plan is in accordance with the internal audit department's terms of reference.

7.8 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.
- 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 prioritize their time – but that's another story.

An example of the quarterly plan is in appendix I

8 The audit

8.1 Objective of the audit

To provide an independent and rational opinion as to whether the organization is likely to achieve the objectives covered by the audit. The processes involved are shown below.

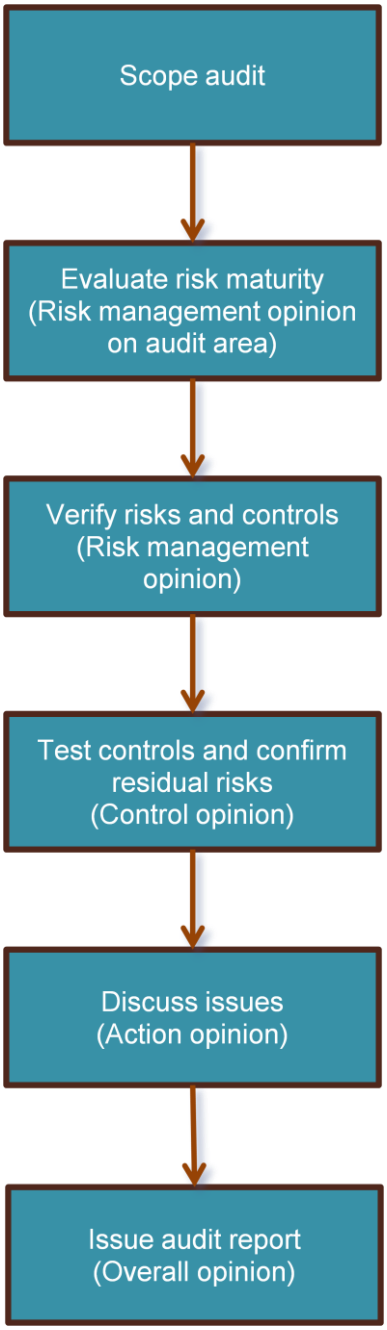


Fig 8. Audit processes

8.2 What is an audit?

8.2.1 The aim of 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 business objectives to which our opinion will refer.

For *each* of the risks threatening our objective(s), the audit should give an opinion on the following questions:

- Has management: specified this objective, identified the risks threatening this objective and established control(s) which should reduce the risk to acceptable levels (and therefore make the achievement of the objective likely)?
- Is the control(s) sufficient and operating to bring the risk to below the risk appetite and ensure the achievement of the related objective?
- If necessary, is action being taken which will bring the risk to below the risk appetite and ensure the achievement of the objective?

The opinion on each risk will determine the opinions given in the report (chapter 2)

8.2.2 The basic structure of an audit

So how do we do the audits? Back to first principles: internal auditing provides an opinion to management whether *objectives* are likely to be achieved based on whether the *risks*, which threaten them, are being managed by *internal controls.* So the basic structure of an audit is as follows: (letters refer to the *Working Papers* spreadsheet (*workingpapers.xlsx*) and associated documents at https://www.internalaudit.biz/webresources/workingpapers.html

A. Plan the audit. This may have to start several months before the audit in order to set up meetings and carry out initial research into the work involved. Inoculations may be required for some overseas audits.

B. Document the information needed to provide an introduction to the departments and processes which will be involved in the audit.

C. Document the scope of the audit and agree this with the management affected (the 'auditees')

D. Discuss the audit with all relevant staff to understand the background to the audit. Are staff frustrated with the systems; do they understand risk; what training do they receive?

E. Check the risk management framework for the functions concerned, using the Risk Maturity Checklist (Appendix F).While the risk maturity should be the same as that for the organization, this may not be true. Where the functions have 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. ('Consultancy' work).

F. Set up the Objectives, Risks and Controls Register from the organization's ORCR.

   - Document all the objectives and associated risks (appendix J and spreadsheet). The definitive list of risks is noted in the column 'risks for this audit'. The more risk mature the organization is, the more information will be available on risks and their associated controls.

- Flowchart the systems in use, sufficient to identify the risks arising from them (for example risks arising from input of data).

G. Test that the internal controls are sufficient and operating to bring the associated risk to below the risk appetite. 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.

H. Decide where risks are not being mitigated to below the organization's risk appetite. Note these as deficiencies. Discuss them with appropriate management and note the action they will take (if any).

I. Write the draft report based on the deficiencies found, providing opinions to management as detailed in chapter 2.

J. Issue the final report.

K. Obtain feedback on the audit process from 'client' management and staff involved. Appraise staff using this feedback.

The practical processes for carrying out an audit are detailed in 'Book 4 - The manual' and the accompanying spreadsheet. The notes below give a brief outline.

8.3 A - Planning

Planning is important for any audit but more important if we are involving managers and staff who have never seen an auditor. Meetings will have to be arranged months before the audit to brief managers about the audit process, while at the same time learning about the state of risk maturity in their department. If this needs improving, now is the time for management to get it done.

The better everyone is prepared, the easier the audit process.

8.4 B - Background information

At the planning stage background information can be assembled which will help with the scoping of the audit. Organization charts can be obtained and the processes which deliver the objectives involved in the audit can be mapped at high level so that the boundaries of the audit work can be decided.

8.5 C - The audit scope

The purpose of the scope document is to set out *why* the audit is being done; *what* objectives, 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 emphasize the monetary value at risk. This could include not only potential losses but also ‘loss of opportunity’.

The scope must state the *objectives* being covered; relating them back to the agreed ORCR. If any objectives 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 also need to note the objectives because our audit will be providing an opinion on the likelihood of the objectives being achieved, based on our audit work.

The scope therefore, will have the following headings:

- The reasons for the audit.
- The objectives, risks and related systems and key controls

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

The reasons for the audit should include the objective of the audit, that is, to provide an opinion on the following primary question.

- Are the organization's objectives likely to be achieved, based on the management of opportunities and risks?

And on two secondary questions:

- Has management established a proper internal control framework? That is, has management: specified their objectives, identified the risks threatening these objectives and established controls which should reduce the risks to acceptable levels?
- Are these controls sufficient and operating to bring the risks to below the risk appetite and ensure the achievement of the related objective?

If the answer to any of the above questions is not 'Yes':

- Is action being taken which will bring the risks to below the risk appetite and ensure the achievement of the objective?

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 (if that hasn't been done as part of planning).

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 and a revised document issued.

8.6 D - Meetings

This section of the working papers includes notes of all meetings up to the writing of the draft report. Detailed minutes of meetings are usually unnecessary but notes of meetings which record important issues raised and decisions made should be typed up and sent to all concerned. This, hopefully, will avoid any misunderstandings about what was decided!

8.7 E - Evaluate risk maturity

Ideally the risk maturity of the function being audited will be the same as the charity's (see worksheet appendix F and the RAU spreadsheet) but this will not necessarily be true, especially in the case of subsidiaries and offices some distance from Head Office which couldn't be visited during the planning stage. Phone calls should be made to discuss the audit planning.

So the risk maturity checklist is completed for the function being audited. If the maturity is found to be risk naïve, aware or defined, the auditors have two options:

- Get the next plane home after instructing management to improve its risk maturity OR

- Work with management to construct an 'Objectives, Risks and Controls Register' for the audit, which we will call the 'Audit database'.

The first is not usually considered desirable, so it has to be the second.

We can now answer the question, 'Has management established a proper internal control framework? That is, has management: specified their objectives, identified the risks threatening these objectives and established controls which should reduce the risks to acceptable levels?'

8.8 F -The audit database (ORCR)

8.8.1 Set-up

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 C), meetings and best practice guidelines.

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

The example in appendix J is for the audit of 'Arrange land transport' (grouped into *Transport of food to famine relief camps*, audit number 146 - see the *workingpapers.xlsx* spreadsheet F).

The risks we identified in level 3 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 *Working Papers* spreadsheet workbook is the central information source for the audit. It contains most of the data related to the audit, and is 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 paper documentation used in a ‘traditional’ audit! If any necessary paper documents need to be filed, they can be scanned in.

Risks that are present in most processes should also be considered (setting of objectives, decision making, lack of training, no contingency planning, poor competencies, fraud – details in appendix K). Some of these have been added into the audit database as examples but in practice, more would need to be included. See also the COSO audit program for tests to be included in each audit, if appropriate.

8.8.2 Determine risks and controls

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

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, are operating controls to manage them and therefore achieving their objectives. If we don’t think we have the expertise to do this, we should be bringing in help from specialists inside, or outside, the organization.

Fieldwork serves two purposes:

- Checking that all risks have been identified. Some risks, particularly those in systems, for example computer input, may only be identified by a detailed systems examination.

- Ascertaining whether the internal controls are sufficient to manage the risks. Two types are noted in the audit database:
  - Direct controls – those that address the risk directly, such as authorization of invoices, bank reconciliations.
  - Monitoring controls – those processes operated by management to ensure key controls are operating effectively, such as approving the bank reconciliations, scrutinizing the overdue debtors' listings.

The internal controls will be noted in the audit database, as will those processes which monitor the proper operation of the controls.

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.

8.9 G - Testing controls

The existence of controls will be checked, paying particular attention to those which have a significant effect on inherent risk; 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 organization. If it is highly mature (risk enabled) we should have the confidence that management has implemented good internal controls and we can concentrate on testing their monitoring of these controls. For a less risk mature organization (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 and therefore achieve objectives. The important question to ask is, "If these controls fail in the future – how will *management* know?"

The managers with whom we are working should be provided with a report showing objectives, risks and controls extracted from the database, and asked to confirm the existence of these controls. This can be done as an appendix to the audit report (appendix L).

8.10 H - Deficiencies

8.10.1 Update reports

We should have kept the managers (of the objectives being audited) informed of progress throughout the audit, particularly if major deficiencies were found. This gives them the opportunity to implement additional controls as soon as possible and avoids nasty surprises at the close down meeting. Circulate notes from these meetings (section D).

8.10.2 Identifying deficiencies

This is the difficult bit – assessing whether the risks are being properly managed by the system of internal control. If not, then the possible deficiency is identified for discussion.

Each residual risk needs to be scored after testing has determined the existence and effectiveness of the control which should be reducing the threat of the risk to the objective.

Having determined the residual risk score, the guide and chart below could assist in coming to an opinion about the risk threat

Guide to reporting residual risks			
Residual risk score	**Report control opinion (see chapter 2)**	**Report as**	**Action**
Greater than15	No	Major deficiency	Immediate action required to bring risk below the risk appetite
Less than 15 greater than 4	Yes with exceptions	Deficiency	Action required to bring risk below the risk appetite
4 or less	Yes	No deficiency	No action required

BUT

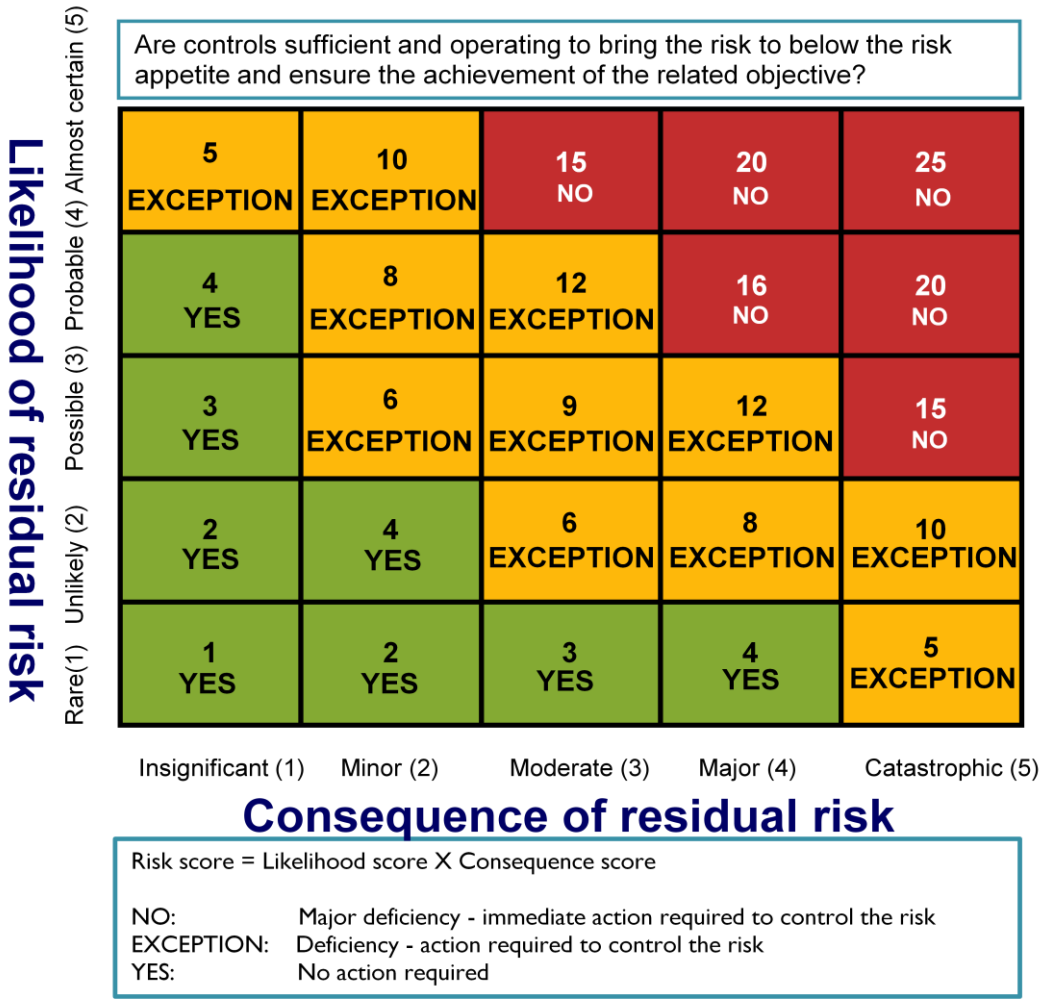
Don't place too much reliance on the scoring! It's a guide not an absolute.

Before you finalize the list of deficiencies, for each risk, ask yourself:

- Am I convinced the control, as specified by management is working?
- Am I able to inform the board/audit committee that the control is sufficient to bring the risk threat to below their risk appetite?
- Will management know if the control fails in the future?

If the answer to any of these questions is **not** a clear 'YES', you must report a deficiency, whatever the risk score (which needs to be changed to reflect your concern).

The risk management community seems skeptical about scoring risks in this way and setting up 'risk appetites'. In my opinion, while such a mechanistic way of assessing the management of risks is not ideal, internal audit has to have some way of measuring the huge number of risks across the organization. Without this measure it would be very difficult to prioritize audits and objectively decide on the audit opinion. Since the work of internal audit may be subject to expectations which have a legal requirement, for example the UK's governance requirements, it may be necessary to demonstrate that internal audit's work is based on rational measurements.



We are now able to form preliminary opinions on the management of each of the risks:

- Has management: specified this objective, identified the risk threatening this objective and established control(s) which should reduce the risk to acceptable levels?
- Is the control(s) sufficient and operating to bring the risk to below the risk appetite and ensure the achievement of the related objective?

Where residual risks are above the risk appetite (opinion = No or Exception), these will be listed for discussion with management (section H). The opinion on each risk will determine the overall conclusions.

8.10.3 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, recorded in section H. 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. One of the advantages of the risk based internal audit is that it shows all the risks which are being properly managed, not only those that are not.

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

Having discussed the deficiencies, those which have a common underlying cause can be combined to make the report shorter and easier to understand.

Where we are reporting 'major deficiencies' or 'deficiencies', should we make recommendations as to how these can be reduced to acceptable risks? Theoretically, since management is 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 organizations, but with risk defined organizations 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.

8.11 I & J - Reporting to management

8.11.1 The report

The opinions provided by the report have been detailed in chapter 2.

How you report your conclusion will depend on your organization and the regulations which apply (COSO etc). 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 spend haggling over the score and not enough time on controlling the risks!

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

- **Summary of conclusions**, showing the objectives covered by the four opinions. Sent to the audit committee, main board directors (or trustees or owners), business directors responsible, managers directly involved.
- **Executive Summary**, containing the introduction to the processes audited. The objective of those processes, brief details of the deficiencies found and conclusions. Circulation as for the summary of conclusions.
- **Major deficiencies**, (these result from red risks) detailing the risk, the consequence if the risk event occurs, the cause, 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.
- **Deficiencies**, (amber risks). Content as for major deficiencies.
- **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.
- **Objectives, risks and controls report** (appendix L). 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.

- It provides managers with a list of objectives, 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.

The report should generally be written (that is, word-processed) as it forms an important record within the organization. However, the contents of the report can be presented, using PowerPoint for example.

8.12 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, providing an opinion to management as to whether 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 an ORCR with possible controls. As the project progresses this should become more detailed, until it resembles the standard ORCR. As with the project risks, we should issue regular monthly reports.

8.13 Summary report to the audit committee

Regulations often require an 'annual report to the board (or Board Audit Committee)' from management on the effectiveness of internal controls. The frequency and contents of the report to the audit committee will depend on internal audit's charter but will normally include:

1. Opinions on whether:

- Objectives are being achieved.
- The significant risks (that is, those above the board's risk appetite) 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 deficiencies in internal control that have been reported.
- Necessary actions are being taken promptly to remedy any major deficiencies.

2. Whether 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).

This summary is very important, since it is one of the main methods that the audit committee will use to judge the competence and worth of internal audit. The CAE should ensure that the audit committee have been consulted on its format and should obtain feedback from each meeting that he/she attends.

9 Pushing out the boundaries

9.1 How the boundaries of internal auditing are changed

We saw in chapter 4 that the boundaries ***to*** which we pushing out internal audit include:

- Providing opinions on the likelihood of objectives being achieved, based on the management of those risks threatening the achievement of all the organization's objectives. (Covered in chapter 7)
- Considered by the board and audit committee as an essential participant in ensuring the organization's objectives are achieved (9.2).
- Regular contact with all senior management (9.3).
- Auditors having a wide range of experience (9.4).

We can only talk about the change brought about by risk based internal auditing 'pushing out the boundaries' if we know what it is changing *from*. That's not easy, since there are many different way of delivering internal auditing at present. We can summarize the changes below, by making some assumptions regarding 'old auditing boundaries':

Audit process	**New auditing boundaries (Objective focused internal auditing)**	**Old auditing boundaries**
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 the organization is likely to achieve its objectives	Confirm internal controls are satisfactory. Improve efficiency
Annual plan	Audits directed at the control of high risks, as defined by management, which are threatening all objectives	Cyclical plan of audits, not necessarily dependent on risk levels linked to objectives, and decided by the CAE.
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 organization	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 using an audit program

RBIA – Pushing out the boundaries

Audit process	New auditing boundaries (Objective focused internal auditing)	Old auditing boundaries
Assessment of risk maturity	Formal assessment using a questionnaire	Not relevant as a measure of risk maturity is not required
Fieldwork	Ensures the organization has identified all its risks, and is controlling them	Based on a set work program, 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 organization.	Confirms the operation of controls – but may not prioritize these in order of importance. May also be directed towards finding errors, however immaterial. May rely on templates.
Report	Provides an opinion to management as to whether the objectives in the area being audited are likely to be achieved	Confirms internal controls are satisfactory and reports where they are not
Recommend-ations	Management has responsibility for deciding on action to be taken. Internal Audit confirms action to be taken will ensure objectives are met.	Recommendations may be made to correct weaknesses found
Annual report to the 'board'	Provide an opinion as to whether objectives are likely to be achieved. 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
Relationship with management	Contact with managers and directors from the whole organization	Contact limited to managers and directors associated with financial audits
Perception of internal audit	Considered by the board and audit committee as an essential participant in ensuring the organization's objectives are achieved.	An 'off-line' control function
Staffing	Self-motivated, experienced staff used to working with senior management. May be specialists who are not accountants or internal auditors, and may be seconded.	Usually accountants and career internal auditors

9.2 Perception of internal audit

Traditional internal audit may have been perceived by the board and audit committee as a 'control' function. An important contributor to the achievement of the organization's objectives but not a major one. By pushing out the boundaries to all the objectives and providing an opinion on the control over the risks threatening them, internal audit should be seen by the board as a major contributor to the organization.

9.3 Relationship with management

One major, positive, impact can be changes in the relationship with management. The traditional audit approach is to notify management that an audit will take place, probably have an initial meeting to discuss the audit and any management concerns over controls. The auditors then carry out their tests and, unless any major deficiencies are found, the next contact with management is a discussion of the deficiencies, with recommendations.

The RBIA new boundary involves management to a far greater extent:

- The risks to be covered in audits will exist in all parts of the organization and audits will therefore involve managers in departments never visited before. Many risks will be very significant to the organization and the discussion of their controls will involve more senior managers and directors than might be involved in traditional finance orientated audits.
- RBIA emphasizes management's responsibility for managing risks. Audits will involve more discussion with managers about their risks and their responses to them. There will be an initial meeting with managers, possibly involving a risk workshop to examine risks in greater depth, and contact throughout the audit to discuss issues.
- The 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 Chief Audit Executive (CAE) / 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.

Audit staff will have to use more 'people' and 'business' skills, such as interviewing, influencing and problem solving. While most audit staff will welcome the opportunity to move away from audit programs to more risk and business based audits, some members of staff may find this move difficult. Training will certainly be required and some staff may have to be transferred.

9.4 Staff expertise

The expansion of the audit universe to cover all risks threatening the organization's objectives requires that the auditor has sufficient knowledge to come to an opinion on the likelihood of achieving objectives, based 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 Sales tax / 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 organization. This might be done on a permanent basis, temporary (a year, for example) or for a specific audit. Such specialists would have to be independent of the area they were auditing. For example, a warehouse manager from one overseas subsidiary could audit warehouse processes in another. Training in the internal audit methodology would have to be provided, and the specialist auditor probably teamed up with an internal auditor.
- We use specialists from outside our organization. For example a health and safety expert to audit our health and safety processes. Although such specialists may work alone, 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.

9.5 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.

9.6 Management of the internal audit department

As we have seen, the audit universe and annual plan is based on objectives, risks and controls defined by management. Thus the internal audit manager (CAE) must work closely with managers and the Risk Management Department, should one exist. This is a major change compared with 'traditional' internal audit, where the CAE often draws up the annual plan from his/her judgment of areas which require auditing before agreeing this with senior management and the Audit Committee (if it is ever formally agreed).

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

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

.

9.7 The benefits

Some benefits of pushing out the boundaries have been considered above. Others are:

- 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 organization and its processes – so no need to define which functions internal auditing should involve – all of them.
- Alongside this simplicity, there is a unity. Any recommendations made, and action decided, can be traced back through controls and risks to the organization'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 an opinion to the board about the "likelihood of achieving the organization's objectives". RBIA ties all aspects of internal auditing together; objectives, risks, controls, tests and reports. The relevance of any test can be seen in relation to the opinion on the entire risk management framework because of the relationships set up in the risk and audit universe. This is not always possible where audit programs are used, as it is not always clear why the test is being carried out; the significance if a control is found to be defective; what risk the control is treating and what objective is being threatened by that risk. RBIA (or Objective Focused Internal Auditing) 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 organization 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 achievement of the most important objectives.
- 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 programs, without really understanding why the test is being done.
- Risk-based auditing is more efficient, because it directs audits at the most important objectives. It therefore covers 'decision' risks which are of greatest interest to the decision-makers and is therefore much more relevant to senior management.
- We can rank action required to improve controls, to provide the greatest value added in terms of objectives achieved.
- RBIA should highlight risks which are over-controlled, and therefore improve efficiency

Fundamentally, the internal audit function is now much more part of the organization and less introspective. It involves the organization 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.

9.8 Disadvantages

With every advantage there are always some disadvantages:

- The closer relationship with the rest of the organization 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 organization, 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.

9.9 Some questions

9.9.1 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 local regulations. 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.

9.9.2 Do I have to throw away my work programs and questionnaires?

Ideally – yes! The danger of using programs, templates and pre-defined questionnaires is:

- They can be incomplete. In particular, they might not check the management of all significant risks.
- Since many are not linked to objectives or 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.

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.

9.9.3 Do financial audits disappear?

No, but the objectives included in these audits have to be judged alongside all the objectives faced by the organization. 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?

9.9.4 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 defense 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:

- Ensure they have clear objectives.
- Help them to identify the significant risks which might prevent them achieving their objectives.
- 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. 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 objective-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 local requirements.

9.9.5 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 organization 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

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 objectives will be met through effective risk management. However, the Board may decide to obtain assurance directly from these departments. The danger of this approach is that risks may fall between the various areas of responsibility.

9.9.6 What about the IIA standards?

The content of the books on the website is intended to be compliant with the latest IIA standards. Appendix M shows which part of the books is relevant to the individual standards (excluding those covering consultancy).

9.9.7 What about the COSO framework?

COSO (www.coso.org) issued an update to 'Internal Control - Integrated Framework' in May 2013. The aim of the document is to inform organizations about the necessary elements of internal control. It is principles-based and must be built into all audits (see appendix K for examples), as opposed to only setting up an annual 'checklist' to ensure compliance.

The website includes an 'audit program' for COSO.

9.9.8 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 recognize this.

Otherwise the detection of fraud is management's responsibility. Similarly, 'embedded monitoring' carried out by the internal audit 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.

10 Glossary

Beware – these are not 'official' definitions!

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

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

Control: 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.

Deficiency: A risk which is not below the residual risk appetite and which, if it occurred, would hinder, but not prevent, the achievement of the objective it is threatening.

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

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

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 organization'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 organization. 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 organization'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.

Major deficiency: A risk which is not below the residual risk appetite and which, if it occurred, would prevent the achievement of the objective it is threatening.

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

ORCR (Objectives, Risks and Controls Register): The complete list of objectives of the organization, with the risks threatening their achievement and the controls intended to bring the risks to below the risk appetite.

Process: a task which assists in delivering an organization's objectives (for example, dispatch of goods), or controls risks (authorization 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 organization as a whole, for different groups of risks or at an individual risk level. Risks above the risk appetite are considered a threat to the reasonable assurance that an organization will achieve its objectives.

Risk and Audit Universe: The ORCR 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 organization understands its risks and is managing them.

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

11 Further reading

11.1 Links

As it difficult to keep links up-to-date and add new information as it becomes available, I am making this available on www.internalaudit.biz.

11.2 You want to manage information or implement computer systems??

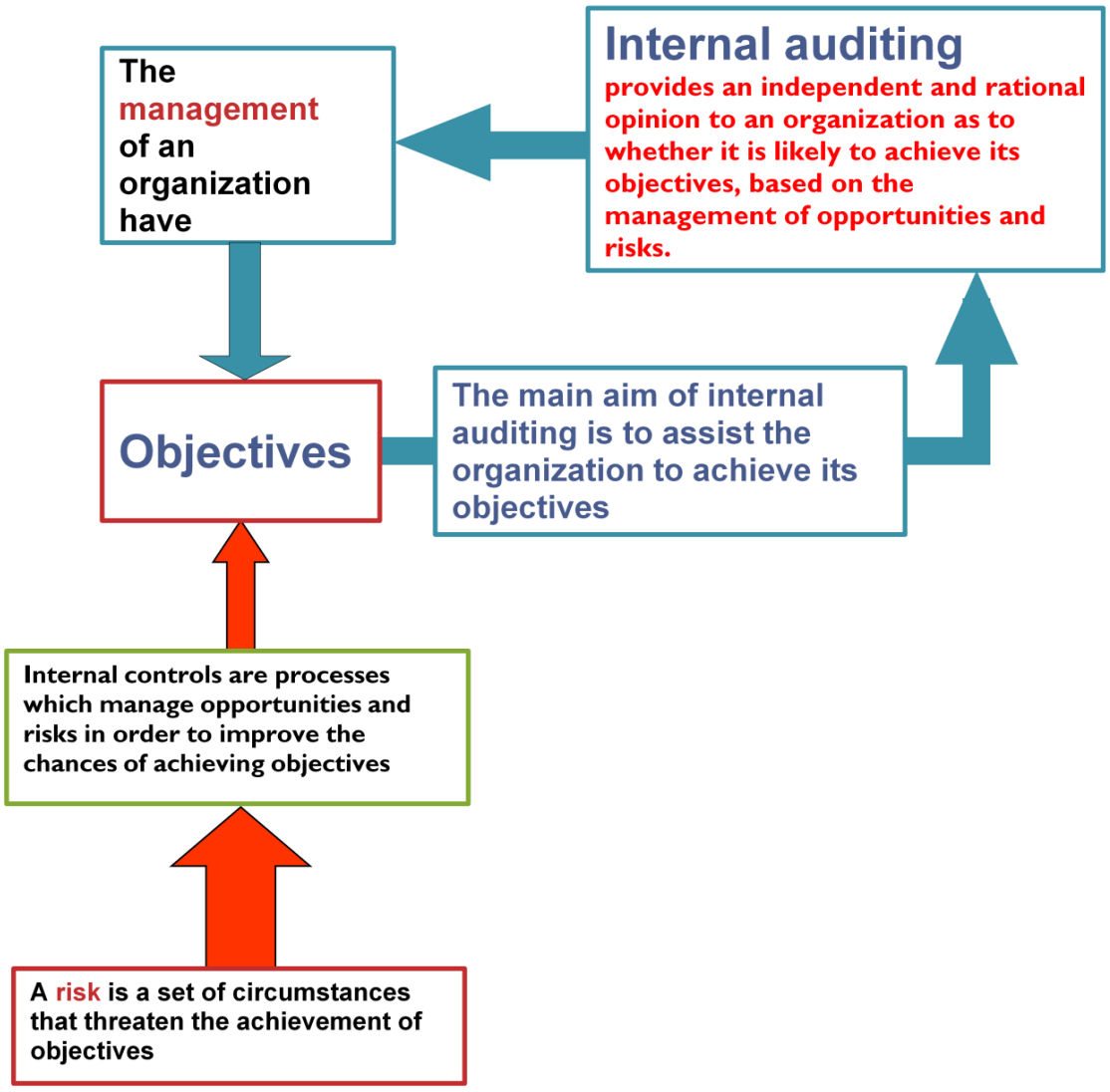
You might like to look at my other sites, which consider the management of information (www.managing-information.org.uk) and Specifying, Choosing and Implementing Computer Systems (http://www.systemsimplementation.co.uk/).

12 Appendices

TOPIC		Original*
Internal auditing objectives	A	Excel
Interviewing tips	B	This doc
Running a risk workshop	C	This doc
Objectives and risks	D	This doc
The ORCR	E	Excel
Assessing the organization's risk maturity	F	Excel
Risk and Audit Universe – Audit planning	G	Excel
Risk and Audit Universe – Audit plan 2014	H	Excel
Quarterly plan	I	Excel
Audit risk database for audit 146	J	Excel
Risks to be considered	K	This doc
Process, risks and controls report	L	This doc
Figures in this document:		Excel

*Excel appendices are in the 'RAU' spreadsheet which may be downloaded from http://www.internalaudit.biz

A Internal auditing objectives



B 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 organization'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 that 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 organization 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.

C 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.

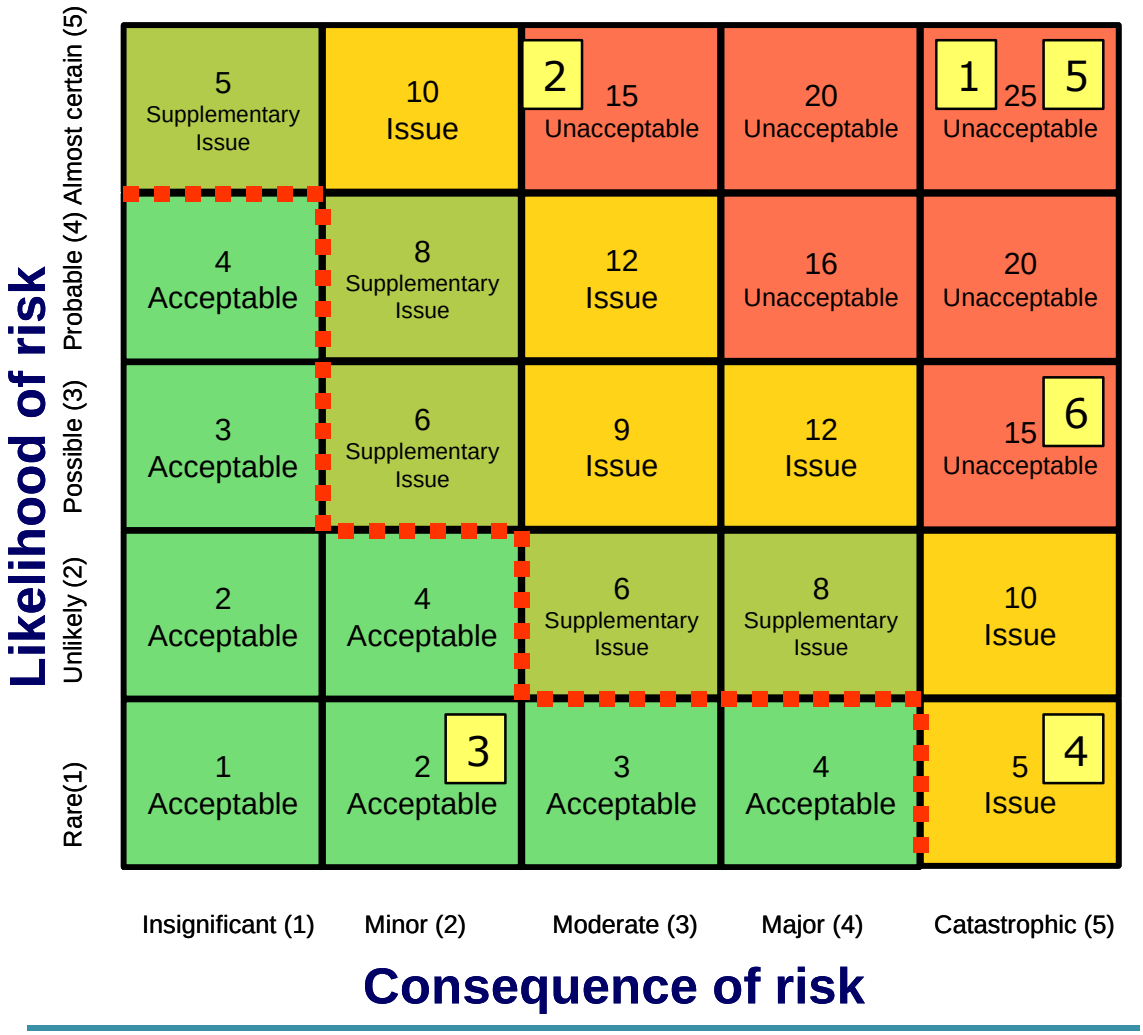
Preparation:

- 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 organization, 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 organization, 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.
- When wording risks, try not to make them just the failure to deliver a process. For example the risk hindering "Organize door to door collections" should not be "Fail to organize door to door collections".
- More importantly risks should not be the absence of a control. For example, the risk "Invoices are not authorized" presupposes a control. The risk is "Invoices may be paid for goods or services not required"; the control is "All invoices are authorized by a senior manager". If a risk occurs a loss *will* result. If there is an absence of a control, a loss will *not necessarily* result.
- 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). You may also be able to use an interactive white board, if one is available.

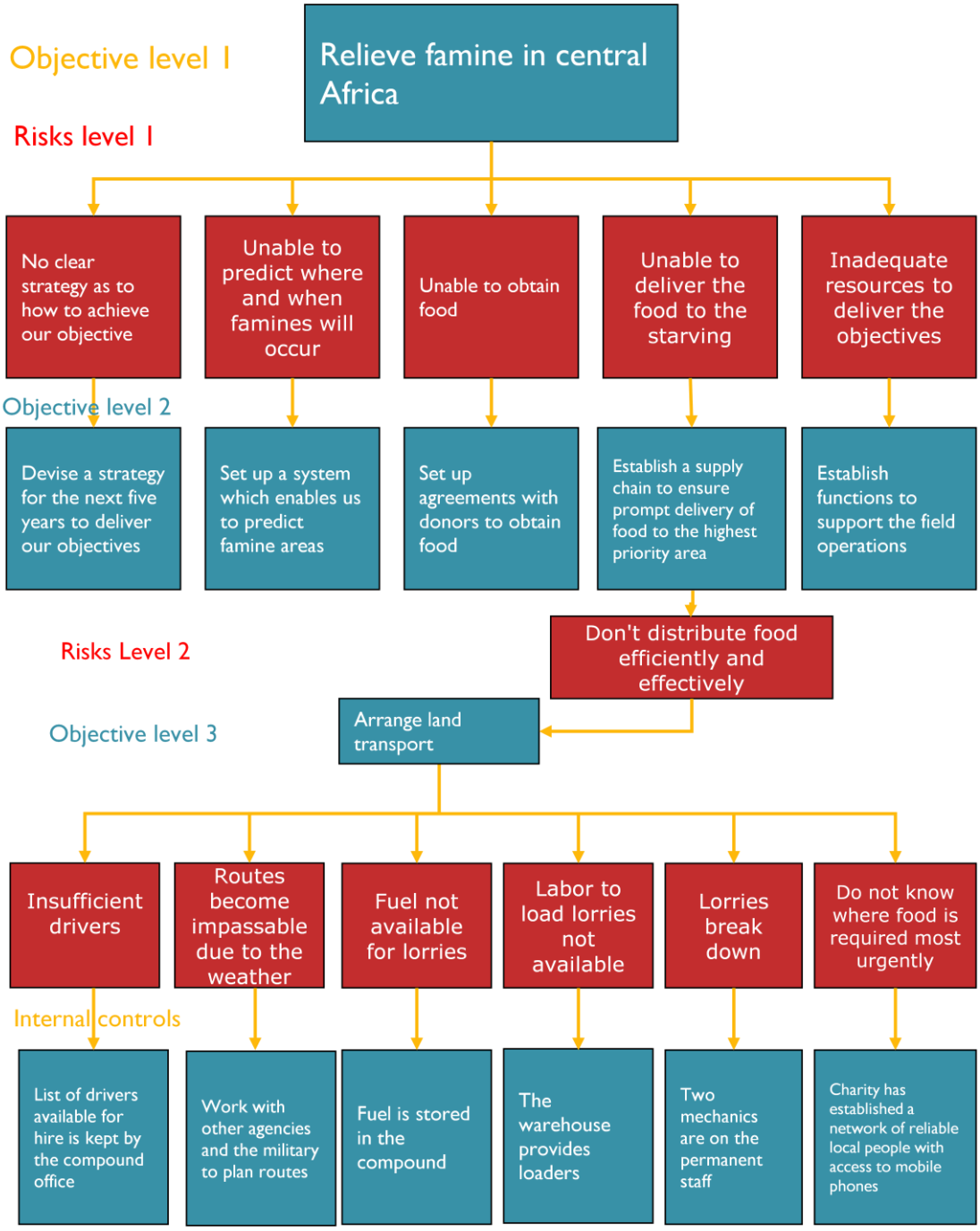


- For each risk, ask the meeting where it fits on the graph. This can be done by writing the number on a 'Post-it' note and sticking on the paper. The advantage of this method is that you can change your mind easily. Whatever you do, write the agreed numbers directly on the paper after the meeting, as the post-it notes fall off when you take it down!
- The absolute score is not as important as the relationship between the risks, that is, which are the most serious.
- Don't be surprised if many of our absolute risks are scored as 25. We are looking at significant risks, with no controls. External risks, such as "Information predicting next year's harvest is not available" may have likelihoods less than high.
- For some risks there is a link between consequence and likelihood. For example take the risk, "lorries may break down". If we have many lorries, we could score this risk as the possibility of all lorries breaking down at once (consequence = very high, likelihood = low) or the possibility of one lorry breaking down (consequence = low, likelihood = very high). Either way the risk score is the same (10). In these circumstances, the risk should be clearly stated.
- 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.

D Objectives and risks



E The ORCR– inherent scores (part only)

Level 1 objective: Relieve famine in central Africa

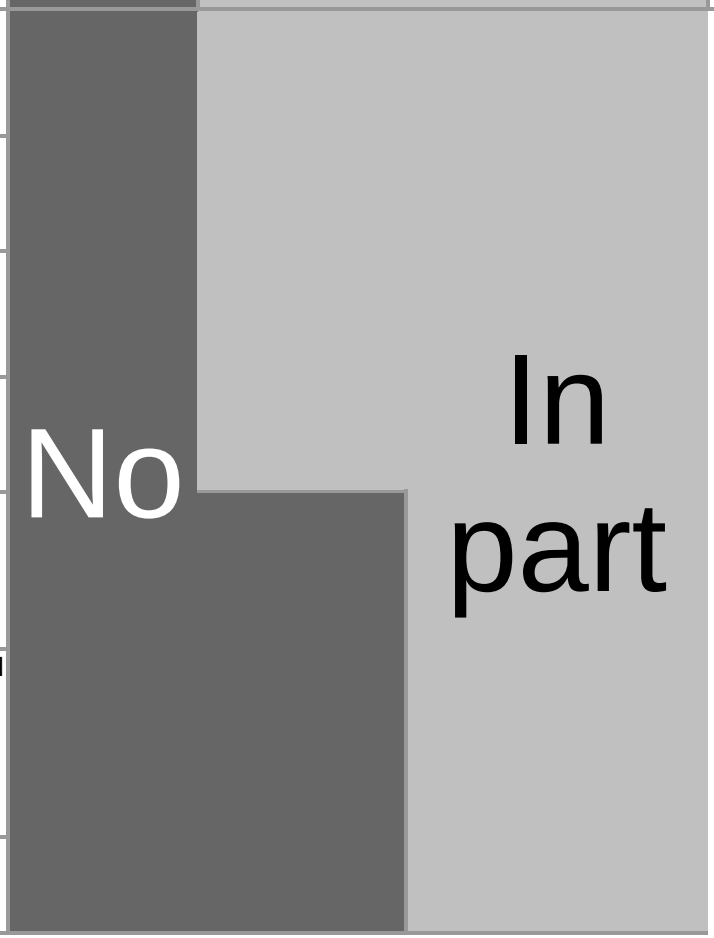
Level 2 objective	L2 Risk	Level 3 objective	Risk (to level 3)	Inherent risks		
				IRC	IRL	IRS
Devise a strategy for the next five years to deliver our objectives	Board do not define a strategy	The trustee's of the charity define the future aims and plans	Management do not support the strategy with the result that it does not achieve its aims	5	5	25
Devise a strategy for the next five years to deliver our objectives	Strategy not communicated	Tell all staff about the strategy and its importance to them	Strategy might not be the best to achieve our objectives	5	5	25
Devise a strategy for the next five years to deliver our objectives	Strategy not put into action	The strategy is converted into targets and action for all staff	People in the organization are unaware of the strategy	5	5	25
Devise a strategy for the next five years to deliver our objectives	Strategy not put into action	The strategy is converted into targets and action for all staff	Charities aims not achieved effectively and efficiently. Possible loss of funds	5	5	25
Devise a strategy for the next five years to deliver our objectives	Strategy not put into action	The strategy is converted into targets and action for all staff	New projects do not add value	5	5	25
Devise a strategy for the next five years to deliver our objectives	Strategy becomes out-of-date	Aims and plans to be regularly updated as circumstance change	Charity does not achieve its objectives because strategy not updated	4	5	20
Predict famine areas	Poor rainfall	Receive weather reports and assess their long term impact	Reliable weather reports not available	4	2	8
Predict famine areas	Inadequate planting	Understand how much planting has been carried out	Planting reports not available or reliable	3	3	9
Predict famine areas	Crops grow badly	Understand what harvest is likely to be, using weather and planting reports	Do not correctly predict harvest	3	3	9
Set up agreements with donors to obtain food	No food available	Monitor availability	Information on food stocks is not available	5	1	5
Set up agreements with donors to obtain food	No orders placed for food to be delivered when required	Order food from donors	Donor countries will not provide food	5	5	25

F Assessing the organization's risk maturity

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

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

	Risk naïve	Risk aware	Risk defined	Risk managed	Risk enabled	Audit test (core IA roles in brackets)
Have all risks been collected into one list? Have risks been allocated to specific job titles?						Examine the 'Risk Universe'. Ensure it is complete, regularly reviewed, assessed and used to manage risks. Risks are allocated to managers. (1)
Have all risks been assessed in accordance with the defined scoring system?						Check the scoring applied to a selection of risks is consistent with the policy. Look for consistency (that is, similar risks have similar scores). (2)
Have responses to the risks (e.g. controls) been selected and implemented?						Examine the risk register to ensure proper controls should be in place. (3)
Have management set up controls to monitor the proper operation of key controls?						For significant risks, examine the control(s) treating it and ensure management would know if the control failed. (5)
Are risks regularly reviewed by the organization?						Check for evidence that a thorough review process is regularly carried out. (1)
Has the risk appetite of the organization been defined in terms of the scoring system?						Check the document on which the controlling body has approved the risk appetite. Ensure it is consistent with the scoring system and has been communicated. (1)
Have management reported risks to directors where responses are not managing the risks to a level acceptable to the board?						For risks above the risk appetite, check that the board has been formally informed of their existence. (4)
Are all significant new projects routinely assessed for risk?						Examine project proposals for an analysis of the risks which might threaten them. (1)



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

G Risk and audit universe for the year 20X1 (part)

As at 1 January 20X1

Level 3 objective	Risk	Inherent risks			Control	Internal control owner	Audit Group	Last Audit		Last audit num	Adjusted inherent score		
		Cons.						Opinion			Gap	Factor	Sig
The board of the charity define the future aims and plans	Management do not support the strategy with the result that it does not achieve its aims	5	5	25	All new board members are carefully recruited to ensure they support the aims and ethics of the charity. They have induction training when starting	Managing Director	A Strategy setting and update	green	20X0	130	1	0..25	6.25
The board of the charity define the future aims and plans	Strategy might not be the best to achieve our objectives	5	5	25	The strategy is set after careful discussion, and a risk analysis by the board	Managing Director	A Strategy setting and update	amber	20X0	130	1	0.5	12.5
The strategy is converted into targets and action for all staff	People in the organization are unaware of the strategy	5	5	25	Managers brief all staff yearly. The strategy is on the intranet. New staff have an induction course.	HR Director	B Strategy Communication	red	20X0	131	1	0.75	18.75
The strategy is converted into targets and action for all staff	Charities aims not achieved effectively and efficiently. Possible loss of funds	5	5	25	HR director meets with all management prior to the setting of targets to discuss the targets which will achieve the objectives	HR Director	C Staff Targets	n/a	never done	never done	n/a	1	25
The strategy is converted into targets and action for all staff	New projects do not add value	5	5	25	All new projects must have a clear purpose, a risk analysis, financial justification using @RISK	Managing Director	D Project Approval	n/a	never done	never done	n/a	1	25
Aims and plans to be regularly updated as circumstance change	Charity does not achieve its objectives because strategy not updated	4	5	20	Board discuss and update strategy at their October meeting	Managing Director	A Strategy setting and update	green	20X0	130	n/a	0.75	18.75
Receive weather reports and assess their long term impact	Reliable weather reports not available	4	2	8	Check web for information available about rainfall	Aid Director	F Famine predicting	n/a	never done	never done	n/a	1	8
Understand how much planting has been carried out	Planting reports not available or reliable	3	3	9	Visit areas involved to talk to farmers	Aid Director	F Famine predicting	n/a	never done	never done	n/a	1	9

H Risk and audit universe – annual plan (part)

As at 31 March 20X1

Risk	Internal control 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
Management do not support the strategy with the result that it does not achieve its aims	Managing Director	A Strategy setting and update	200	Strategy setting and update	30	Q2	Khan	scope	6 June 20X1	
Strategy might not be the best to achieve our objectives	Managing Director	A Strategy setting and update	200	Strategy setting and update		Q2	Khan	scope	6 June 20X1	
People in the organization are unaware of the strategy	HR Director	B Strategy Communication	201	Strategy Communication	21	Q2	Smith	To start	29 June 20X1	
Charities aims not achieved effectively and efficiently. Possible loss of funds	HR Director	C Staff Targets	202	Staff targets	10	Q1		Complete	20 March 20X1	21-Mar-06
New projects do not add value	Managing Director	D Project Approval	203	Project Approval	17	Q2	Doe	To start	20 June 20X1	
Charity does not achieve its objectives because strategy not updated	Managing Director	A Strategy setting and update	200	Strategy setting and update		Q2	Khan	scope	6 June 20X1	

I Quarterly plan (part)

As at 3 April 20X1

			Original	Planned	14	15	16	17	18	19	20	21	22	23
Name	**No**	**Audit**	**Budget**	**now**	31-Mar	07-Apr	14-Apr	21-Apr	28-Apr	05-May	12-May	19-May	26-May	02-Jun
Smith		Annual and Bank holidays				1	1		1				1	
Smith	204	Food donations	20	15	4	3	3	4		1				
Smith	210	Security of assets	20	18	1		1	1	3	4	3	4		1
Smith	201	Strategy Communication	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	208	Corporate Social Responsibility	30	5	4		1							
Doe	205	Purchases	25	18	1	3	2	4	4	3		1		
Doe	203	Project approval	17	17			1			1	4	4	2	4
Doe	209	Investments	17	17				1		1	1		2	1
Doe	211	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	207	Corporate Governance	30	5	4		1							
Khan	200	Strategy setting and update	30	27	1		2	5	4	5	5	4		1
Khan	213	Recruitment	20	16			1					1	3	4
Khan	214	Street collections	10	8									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									

J Audit database (146 Transport of food to camps) (part)

Level 3 Risk (from RAU)	**Level 4 Objective** (from audit)	**Risk for this audit**	**Control**	**Tests**	**Result**	Do internal controls, including monitoring controls, reduce risks to acceptable levels?	Is action being taken to promptly remedy deficiency?	**Report reference**
Insufficient drivers available	Hire drivers	Drivers not available	List of drivers available for hire is kept by the compound office	Checked list. It is not regularly updated	Drivers may not be available	**no**	yes	**1**
Insufficient drivers available	Hire drivers	Drivers not properly qualified	Drivers documents are checked and copies made	Checked copies exist.	Documents could be forged	yes		n/a
Routes become impassable due to the weather	Plan route	Route is blocked	Work with other agencies and the military to plan routes	Check the last plan. Examine dates of collection and delivery	HQ also tries to plan routes	yes		**5**
Routes become impassable due to bandits	Plan route	Route is dangerous	The army escorts convoys	Ask drivers and supervisor about escorts	None - escorts are provided	yes		n/a

This is only part of the audit database. It should be downloaded from www.internalaudit.biz (Book 1 spreadsheet 146workingpapers)

K Risks to be considered

The following key process and decision 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/ *Audit test*
Defining strategy/setting objectives	
The governing body has no, or ill-defined, objectives	The governing body (the 'board') has formally approved the organization's objectives
The objectives do not maximize the potential of the organization	All possible options for maximizing potential considered and measured by balancing opportunities against accompanying risks
Objectives have been communicated to all staff	Objectives have been communicated to all staff.
Staff are unaware of their own objectives	All staff should have job descriptions which define their objectives
Staff are unaware what decisions they are required to make to achieve their objectives	All staff should have job descriptions which detail the decisions they may have to make, both to manage risks and to seize opportunities. Where appropriate, stretching but achievable targets should be set for the achievement of objectives
Staff are unaware when they are required to make to achieve their objectives	
Decision Making to achieve objectives	
Authority	
Decisions made at an inappropriate level of staff	The board and senior management should have defined authority levels, including financial if appropriate, for all staff.
Decision making process	
The reason a decision is required is unclear	The decision-makers document the nature of the problem, why a decision is required, and what they are trying to achieve
Incorrect decisions made	Everybody whose information and insight into the situation and the effects of a decision should participate. Rules which define certain courses of action are understood.
Insufficient data is available to make an informed decision	As far as is practical within the time available, decisions should be based on reliable, complete and accurate, current, and timely information.
Decisions are delayed	Decision-makers clearly understand any time limits which might apply

Risk	Possible controls/ *Audit test*
Not all possible choices are identified	All possible alternatives should be identified by the decision-makers and their potential effects on success understood.
Some benefits and threats may not be identified, or their effects not thoroughly evaluated	Consideration should be given to both the potential for harm and the opportunity for reward, recognizing that there may be both multiple 'risks' and multiple 'opportunities', with reliable analysis, including financial modeling, that weighs all the pros and cons in a disciplined manner. For major decisions: an independent check of the process, including any financial case.
Training	
Staff do not understand their role in decision making	Induction training when taking up a new job should include the decisions the job requires
Staff do not understand how to identify choices when making a decision	Formal training courses for all staff covering: ➢ Decisions they need to make and when ➢ The importance of identifying decisions which provide opportunities ➢ How to identify options and evaluate these ➢ When to involve more senior management ➢ Factors which influence their decision making
Staff and their advisors do not allow for their cognitive and other biases that may influence their decisions	
The principles of decision-making are not applied	Formal reporting by management that they have implemented the principles Check of principles to be included in all audits
Fraud	
Assets could be removed from the company	Physical controls (for example a safe)
	Preventive controls (for example division of duties, authorization 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, especially on making decisions	Appropriate training courses available, including scenarios when urgent decisions

Risk	Possible controls/ *Audit test*
	must be made
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
Information	
Information required for decision-making is incomplete or inaccurate	Consider what information might be required to make decisions, often at very short notice and ensure it is available

COSO (Part only)	
Board of directors act irresponsibly)	Sets the tone at the top - The board of directors and management at all levels of the entity demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control *During audit work, consider if any weaknesses in internal control result from directors and management's failure to support integrity and ethical values*
Directors fail to recognize their responsibilities, or delegate them	Guide, direct and review the development and performance of the system of internal control. *Control environment: During audits ensure that integrity and ethical values, structure, authority and responsibility, competence and accountability are present in the parts of the organization being audited*
	Risk Assessment: During audits ensure that directors are reviewing and commenting on management's assessment of risks to the achievement of objectives, including the potential impact of significant changes, fraud and management override of internal control
	Control Activities: During audits check for guidance to senior management around the selection, development and deployment of control activities
	Information and communication: During audits check that the board is obtaining, reviewing and discussing information relating to the organization's achievement of objectives
	Monitoring activities: During audits check that the board assesses and oversees the nature and scope of monitoring activities and management's evaluation and remediation of deficiencies
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.	

L Transport of food - objectives, risks and controls report (part)

Level 4 Objective	Risk for this audit	Control (after action taken to correct deficiencies)
(from audit)		
Receive instructions from country office	Instructions not received	Country office confirms receipt.
Receive instructions from country office	Instructions are late	No controls at HQ to ensure instructions are sent on time
Hire drivers	Drivers not available	List of drivers available for hire is kept by the compound office
Hire drivers	Drivers not properly qualified	Drivers documents are checked and copies made
Plan route	Route is blocked	Work with other agencies and the military to plan routes
Plan route	Route is dangerous	The army escorts convoys
Arrange to collect food	No food available!	HQ arrange for food to available in the warehouses
Load fuel	Fuel not available for lorries	Fuel is stored in the compound
Load food	No loaders	The warehouse provides loaders

IIA Standards (©IIA-Inc)	Web site	Book	Reference
Mission statement			
To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight	The entire risk based internal audit process detailed in the books is aiming to fulfill this mission	All	
Principles			
1. Demonstrates integrity. 2. Demonstrates competence and due professional care. 3. Is objective and free from undue influence (independent). 4. Aligns with the strategies, objectives, and risks of the organization. 5. Is appropriately positioned and adequately resourced. 6. Demonstrates quality and continuous improvement. 7. Communicates effectively. 8. Provides risk-based assurance. 9. Is insightful, proactive, and future-focused. 10. Promotes organizational improvement	Principles 1, 2, 3, 4, and 5 are outside the scope of this website. 6. The audit manual contains instructions on quality control over an audit. 7. The introduction emphasizes the importance of working with management, since they have the responsibility for determining risks.. The audit manual has instructions throughout on keeping management informed of audit progress. 8. The aim of the individual audit process is to provide an opinion on risk management and the achievement of objectives which can be combined with opinions from other audits to provide an overall conclusion given to the board and audit committee. 9 & 10. The aim of the ideas on this website is to be challenging, future-focused and promote organizational improvement.	Book 4 Book 1 Book 4 Book 1 Book 4	K Chapter 2 J
The standards			
The attribute standards	These standards address the attributes of organizations and individuals performing internal auditing. They are outside the scope of the website.		

2000 - Managing the Internal Audit Activity The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.	The ideas on the website should add value by providing opinions on the management of all risks threatening the organization's objectives	All books	
2010 - Planning The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.	One of the website's aims is to demonstrate how to establish a risk-based audit plan.	Book 2 Book 1	 Chapter 7
2010.A1 - The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.	The website advocates the establishment of an annual plan, constantly updated with new risks as recognized by management.	Book 1 Book 2	3.9.3, 7.6 Chapter 5
2010.A2 - The chief audit executive must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions.	The annual plan is sent to the audit committee. Scopes for each audit are sent to appropriate senior management	Book 1 Book 4	7.3, 7.7 C
2020 - Communication and approval The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations.	The annual plan is sent to the audit committee. The resources required are based on the plan. The CAE will inform the audit committee if sufficient resources are not available.	Book 1 Book 1	7.3, 7.7 7.5
2030 - Resource Management The chief audit executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.	The resources required are based on the plan. Expertise may have to be brought in.	Book 1 Book 1 Book 3	7.5 9.4 3.5.4
2040 - Policies and Procedures The chief audit executive must establish policies and procedures to guide the internal audit activity.	The manual sets down appropriate procedures for individual audits. Other policies and procedures are outside the scope of the website.	Book 4	

2050 - Coordination The chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.	The CAE will need to liaise with any 'Risk Management' function. The board will need to define the responsibilities of functions responsible for risk, such as Health and Safety and Quality Control.	Book 2 Book 3	1.2 2.3
2060 - Reporting to Senior Management and the Board The chief audit executive must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan and on its conformance with the Code of Ethics and the *Standards*. Reporting must also include significant risk and control issues, including fraud risks, governance issues, and other matters that require the attention of senior management and/or the board..	A summary report will be sent to the audit committee.	Book 1	8.13
2070 - External Service Provider and Organizational Responsibility for Internal Auditing When an external service provider serves as the internal audit activity, the provider must make the organization aware that the organization has the responsibility for maintaining an effective internal audit activity	Not included		
2100 - Nature of Work The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact.	The books on the website aim to do this.		

2110 - Governance The internal audit activity must assess and make appropriate recommendations to improve the organization's governance processes for: ➢ Making strategic and operational decisions. ➢ Overseeing risk management and control. ➢ Promoting appropriate ethics and values within the organization. ➢ Ensuring effective organizational performance management and accountability. ➢ Communicating risk and control information to appropriate areas of the organization. ➢ Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management.	The first three bullet points are included within the Objectives, Risk and Controls Register (ORCR) and individual audits. The first bullet point is included in Book 2's ORCR: Level 2 strategic objective, 'Establish clear codes of conduct to be followed by all staff (includes the board)' The second and third bullet points are included in all audits. The fourth bullet point is not addressed in the website.	Book2	ORCR
2110.A1 - The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.	Included in the ORCR Strategic Objectives	Book 2	ORCR
2110.A2 - The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.	Included in the ORCR and each audit	Book 2 Book 4	ORCR ORCR
2120 - Risk Management The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.	The risk maturity of the organization is assessed before audit planning and as part of each audit.	Book 1 Book 4	5, 8.7 E

2120.A1 - The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the: • Achievement of the organization's strategic objectives; • Reliability and integrity of financial and operational information; • Effectiveness and efficiency of operations and programs; • Safeguarding of assets • Compliance with laws, regulations, policies, procedures, and contracts	Covered by each audit	Book 4	ORCR
2120.A2 - The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.	Covered by each audit	Book 4	ORCR
2130 - Control The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.	Covered by each audit	Book 4	ORCR
2130.A1 - The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the: • Achievement of the organization's strategic objectives; • Reliability and integrity of financial and operational information; • Effectiveness and efficiency of operations and programs; • Safeguarding of assets • Compliance with laws, regulations, policies, procedures, and contracts	Covered by each audit	Book 4	ORCR

2200 - Engagement Planning Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement.	Included in the scope for an individual audit.	Book 4	A, C
2201 - Planning Considerations In planning the engagement, internal auditors must consider: • The strategies and 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 governance, risk management, and control processes compared to a relevant framework or model • The opportunities for making significant improvements to the activity's governance, risk management, and control processes.	The audit is planned from the Risk and Audit Universe which includes consideration of these points. These points are Included in the scope for an individual audit.	Book 1 Book 2 Book 4	Chapter 3 Chapter 2 A, C
2201.A1 - When planning an engagement for parties outside the organization, internal auditors must establish a written understanding with them about objectives, scope, respective responsibilities, and other expectations, including restrictions on distribution of the results of the engagement and access to engagement records	Not included		
2210 - Engagement Objectives Objectives must be established for each engagement	Done as part of the annual planning which is derived from the organization's objectives. Then each audit has an agreed scope	Book 1 Book 4	Chapter 7 C

2210.A1 - Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.	Done as part of the annual planning which is derived from the organization's objectives. Then each audit involves gathering background information.	Book 1 Book 4	Chapter 7 B
2210.A2 - Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.	Included in the audit if considered above the risk appetite	Book 4	B, C
2210.A3 - Adequate criteria are needed to evaluate governance, risk management, and controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must identify appropriate evaluation criteria through discussion with management and/or the board.	The risk maturity of the organization is assessed before audit planning and as part of each audit.	Book 1 Book 4	5, 8.7 E
2220 - Engagement Scope The established scope must be sufficient to achieve the objectives of the engagement	The scope is approved by the CAE and agreed with management.	Book 4	C
2220.A1 - The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.	The scope will consider these where the risk is above the risk appetite	Book 4	C
2220.A2 - If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards.	Not included		

2230 - Engagement Resource Allocation Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.	Resources are decided as part of the annual planning process. Resources are allocated in the quarterly plan.	Book 1 Book 1	7.5 7.8
2240 -Engagement Work Program Internal auditors must develop and document work programs that achieve the engagement objectives.	The manual details these procedures to be used during an audit.	Book 4	All
2240.A1 **–** Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement. The work program must be approved prior to its implementation, and any adjustments approved promptly.	The manual details these procedures to be used during an audit.	Book 4	All
2300 - Performing the Engagement Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.	The manual details these procedures to be used during an audit.	Book 4	B, E, F, G, H
2310 - Identifying Information Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives	The manual details these procedures to be used during an audit.	Book 4	B, E, F, G, H
2320 - Analysis and Evaluation Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.	The manual details these procedures to be used during an audit.	Book 4	F, G, H, I, J
2330 – Documenting Information Internal auditors must document sufficient, reliable, relevant, and useful information to support the engagement results and conclusions.	The manual details the procedures to be used during an audit.	Book 4	
2330.A1 - The chief audit executive must control access to engagement records. The chief audit executive must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.	Not included		

2330.A2 - The chief audit executive must develop retention requirements for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.	Not included		
2340 - Engagement Supervision Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.	Reviews are required during individual audits	Book 4	K1-K5
2400 - Communicating Results Internal auditors must communicate the results of engagements.	Meetings and reports used to communicate findings	Book 1 Book 4	8.10, 8.11 H, I, J
2410 - Criteria for Communicating Communications must include the engagement's objectives, scope, and results.	Report includes these	Book 4	J
2410.A1 – Final communication of engagement results must include applicable conclusions, as well as applicable recommendations and/or action plans. Where appropriate, the internal auditors' opinion should be provided. An opinion must take into account the expectations of senior management, the board, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information.	Report is headed by opinions, supported by proper evidence.	Book 1 Book 4	Chapter 2 J
2410.A2 - Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.	Report shows a percentage for risks which are properly controlled which demonstrates the performance of management and staff.	Book 4	J
2410.A3 - When releasing engagement results to parties outside the organization, the communication must include limitations on distribution and use of the results.	Not included		
2420 - Quality of Communications Communications must be accurate, objective, clear, concise, constructive, complete, and timely	The manual is based on these qualities.	Book 4	

2421- Errors and Omissions If a final communication contains a significant error or omission, the chief audit executive must communicate corrected information to all parties who received the original communication.	Not included		
2430 - Use of "Conducted in Conformance with the International Standards for the Professional Practice of Internal Auditing" Indicating that engagements are "conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*" is appropriate only if supported by the results of the quality assurance and improvement program.	Not included		
2431 - Engagement Disclosure of Nonconformance When nonconformance with the Code of Ethics or the *Standards* impacts a specific engagement, communication of the results must disclose the:: • Principle or rule of conduct of the Code of Ethics or *Standard(s)* with which full conformance was not achieved; • Reason(s) for nonconformance; and • Impact of nonconformance on the engagement and the communicated engagement results.	Not included		
2440 - Disseminating Results The chief audit executive must communicate results to the appropriate parties.	The CAE approves the scope which contains the circulation list	Book 4	C
2440.A1 - The chief audit executive is responsible for communicating the final results to parties who can ensure that the results are given due consideration.	The CAE approves the final report and signs the 'Milestones' document as evidence	Book 4	A1

2440.A2 - If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the organization the chief audit executive must: • Assess the potential risk to the organization; • Consult with senior management and/or legal counsel as appropriate; and • Control dissemination by restricting the use of the results.	Not included		
2450 - Overall Opinions When an overall opinion is issued, it must take into account the strategies, objectives, and risks of the organization; and the expectations of senior management, the board, and other stakeholders. The overall opinion must be supported by sufficient, reliable, relevant, and useful information.	The overall opinion in the report is supported by further details which can be easily traced back to supporting documentation.	Book 4	J
2500 - Monitoring Progress The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.	The ORCR contains details of the deficiencies and the status of follow-up audits	Book 4	Spreadsheet F
2500.A1 - The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.	Follow-up audits are part of the auditing process detailed in the manual	Book 4	L
2600 - Communicating the Acceptance of Risks When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board	Not specifically included but the audit report would communicate this	Book 4	

RBIA - 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-2004	Link to David McNamee site added
2.0.0	6-Oct-2005	Major revision.
2.0.2	30-Jan-2006	Changes made to take account of IIA Guidance Note
2.0.3	15-Mar-2006	Minor changes
3.0	28-May-2013	Processes renamed as 'Objectives' or 'systems' depending on the context in order to simplify the classification of risks. References to regulations removed, as these change over time.
3.1	1-Jan-2015	Changes made to section 2.4 to align book 1 and 2. Mind map added. Other changes made as a result of new mind map
3.2	21-Feb-2015	Reorganization of section 2 on risk to make it more logical and incorporate sections of book 3 to remove duplication. Updated appendices.
4	4-May-2015	Added section on audit opinion and rearranged chapters to emphasize two parts to the audit process
4.1	12-May-2015	Working papers added as spreadsheet and documents. Book 1 updated to include more details of audit work to correspond to the working papers. Heat maps changed to reflect opinion. (This version not issued)

4.2	26-May-2015	Concept of 'internal audit: expanding the boundaries' introduced. Changes to incorporate publication of revised Book 4
4.3	4-Jun-2015	Includes appendix M and question about compliance with the IIA standards
4.4	8-July-2015	Appendix M updated for changes in the final IPPF
5.0	5-May-2019	Major revision to include opportunities as well as risks; process and decision risks; and to emphasize more on objectives
6.0	7-May-2020	Revision to drop risk based and concentrate on internal auditing. More on decsion-making

End of Book 1